Power Systems

Hardware Management Console installieren und konfigurieren

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Sicherheitshinweise” auf Seite v, „Bemerkungen” auf Seite 103, im Handbuch *IBM Systems Safety Notices* (IBM Form G229-9054) und im *IBM Environmental Notices and User Guide* (IBM Form Z125–5823) gelesen werden.

Diese Ausgabe bezieht sich auf IBM® Hardware Management Console Version 9, Release 2, Wartungsstufe 950, und alle nachfolgenden Releases und Modifikationen, bis dieser Hinweis in einer Neuausgabe geändert wird.

Inhaltsverzeichnis

Sicherheitshinweise

Dieses Buch kann Sicherheitshinweise enthalten:

- Der Hinweis **Gefahr** macht auf eine Situation aufmerksam, die zu schweren Verletzungen von Personen oder zum Tod führen kann.
- Der Hinweis **Vorsicht** macht auf eine Situation aufmerksam, die zu einer Personengefährdung führen kann.
- Der Hinweis **Achtung** macht auf mögliche Probleme aufmerksam, durch die Programme, Geräte, Systeme oder Daten beschädigt werden können.

Sicherheitsinformationen

In Deutschland müssen Sicherheitshinweise, die in einer Veröffentlichung enthalten sind, in deutscher Sprache vorliegen. Eine Dokumentation mit Sicherheitsinformationen liegt dem mit dem Produkt gelieferten Veröffentlichungspaket bei (z. B. Hardcopydokumentation, auf DVD oder als Teil des Produkts). Sie enthält die Sicherheitshinweise in Deutsch und den Verweis, aus welchem englischen Handbuch die Informationen stammen. Vor der Installation, Wartung oder Inbetriebnahme dieses Produkts anhand einer englischen Veröffentlichung müssen Sie zunächst die zu der jeweiligen Veröffentlichung gehörenden deutschen Sicherheitshinweise der betreffenden Dokumentation lesen. Zudem sollte diese Dokumentation bei Verständnisschwierigkeiten in Bezug auf die Sicherheitsinformationen in der englischen Veröffentlichung herangezogen werden.

Ein Ersatzexemplar oder weitere Kopien der Dokumentation mit Sicherheitsinformationen können über die IBM Hotline unter der Telefonnummer 1-800-300-8751 angefordert werden.

Sicherheitsinformationen für Deutschland

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

Informationen zur Lasersicherheit

IBM Server können glasfaserbasierte E/A-Karten oder Features enthalten, die Laser oder Anzeigen verwenden.

Lasersicherheit

IBM Server können innerhalb oder außerhalb eines IT-Racks installiert werden.

Gefahr: Beim Arbeiten am System oder um das System herum müssen die folgenden Vorsichtsmaßnahmen beachtet werden:

Elektrische Spannung und elektrischer Strom an Netz-, Telefon- oder Datenleitungen sind lebensgefährlich. Um das Risiko eines elektrischen Schlags zu vermeiden: Diese Einheit nur mit dem von IBM bereitgestellten Netzkabel an den Versorgungsstromkreis anschließen, sofern IBM ein Netzkabel bereitgestellt hat. Das von IBM bereitgestellte Netzkabel für kein anderes Produkt verwenden. Netzteile nicht öffnen oder warten. Bei Gewitter an diesem Gerät keine Kabel anschließen oder lösen. Ferner keine Installations-, Wartungs- oder Rekonfigurationsarbeiten durchführen.

- 
Dieses Produkt kann mit mehreren Netzkabeln ausgestattet sein. Alle Netzkabel abziehen, um gefährliche Spannungen zu verhindern. Bei Wechselstrom alle Netzkabel von der Netzsteckdose abziehen. Bei Racks mit einem Gleichstromverteiler die Gleichstromquelle des Kunden vom Stromverteiler trennen.

- Beim Anschließen des Produkts an den Strom sicherstellen, dass alle Netzkabel ordnungsgemäß angeschlossen sind. Bei Racks mit Wechselstrom alle Netzkabel an eine vorschriftsmäßig angeschlossene Netzsteckdose mit ordnungsgemäß geerdetem Schutzkontakt anschließen. Sicherstellen, dass die Steckdose die richtige Spannung und Phasenfolge ausgibt, wie auf dem Systemtypenschild angegeben. Bei Racks mit einem Gleichstromverteiler die Gleichstromquelle des Kunden an den Stromverteiler anschließen. Sicherstellen, dass beim Anschließen der Gleichstrom- und Wechselstromverkabelung die richtige Polarität verwendet wird.
- Alle Geräte, die an dieses Produkt angeschlossen werden, an vorschriftsmäßig angeschlossene Netzsteckdosen anschließen.
- Die Signalkabel nach Möglichkeit nur mit einer Hand anschließen oder lösen.
- Geräte niemals einschalten, wenn Hinweise auf Feuer, Wasser oder Gebäudeschäden vorliegen.
- Die Maschine erst dann einschalten, wenn alle Sicherheitsrisiken behoben wurden.
- Bei Durchführung einer Maschineninspektion: Immer annehmen, dass ein elektrisches Sicherheitsrisiko besteht. Alle in dieser Anweisung zur Installation des Subsystems angegebenen Durchgangs-, Erdungs- und Stromversorgungsprüfungen ausführen, um sicherzustellen, dass die Maschine die Sicherheitsbestimmungen erfüllt. Die Maschine erst dann einschalten, wenn alle Sicherheitsrisiken behoben wurden. Vor dem Öffnen des Gehäuses, sofern in den Installations- und Konfigurationsbeschreibungen keine anderslautenden Anweisungen enthalten sind: Die angeschlossenen Wechselstromkabel abziehen, die entsprechenden Sicherungsautomaten im Stromverteiler des Racks ausschalten und die Verbindung zu allen Telekommunikationssystemen, Netzen und Modems trennen.
- Zum Installieren, Transportieren und Öffnen der Abdeckungen des Produkts oder der angeschlossenen Einheiten die Kabel gemäß den folgenden Prozeduren anschließen und abziehen.

  Kabel lösen: 1) Alle Einheiten ausschalten (außer wenn andere Anweisungen vorliegen). 2) Bei Wechselstrom die Netzkabel aus den Steckdosen ziehen. 3) Bei Racks mit einem Gleichstromverteiler die Sicherungsautomaten am Stromverteiler ausschalten und die Stromversorgung über die Gleichstromquelle des Kunden unterbrechen. 4) Die Signalkabel von den Buchsen abziehen. 5) Alle Kabel von den Einheiten abziehen.

  Anschließen der Kabel: 1) Alle Einheiten ausschalten (außer wenn andere Anweisungen vorliegen). 2) Alle Kabel an die Einheiten anschließen. 3) Die Signalkabel an die Buchsen anschließen. 4) Bei Wechselstrom die Netzkabel an die Steckdosen anschließen. 5) Bei Racks mit einem Gleichstromverteiler die Stromversorgung über die Gleichstromquelle des Kunden wiederherstellen und die Sicherungsautomaten am Stromverteiler einschalten. 6) Die Einheiten einschalten.
-  Scharfe Kanten, Ecken oder Scharniere im System oder um das System herum. Bei der Handhabung von Geräten vorsichtig vorgehen, um Schnitte, Kratzer und Quetschungen zu vermeiden. (D005)

(R001 Teil 1 von 2):

Gefahr: Die folgenden Vorsichtsmaßnahmen beachten, wenn an einem IT-Racksystem oder um ein IT-Racksystem herum gearbeitet wird:

- Schwere Einheit – Gefahr von Verletzungen oder Beschädigung der Einheit bei unsachgemäßer Behandlung.
- Immer die Ausgleichsunterlagen des Rackschranks absenken.
- Immer Stabilisatoren am Rackschrank anbringen (falls vorhanden), es sei denn die Zusatzeinrichtung für Erdbeben muss installiert werden.
- Um gefährliche Situationen aufgrund ungleichmäßiger Belastung zu vermeiden, die schwersten Einheiten immer unten im Rackschrank installieren. Server und optionale Einheiten immer von unten nach oben im Rackschrank installieren.
- In einem Rack installierte Einheiten dürfen nicht als Tische oder Ablagen missbraucht werden. Keine Gegenstände auf die in einem Rack installierten Einheiten legen. Außerdem nicht an in ei-

nem Rack installierte Einheiten anlehnen und diese Einheiten nicht zur Stabilisierung Ihrer Position verwenden (z. B. bei der Arbeit auf einer Leiter).

- Gefahr bezüglich Stabilität:
  - Das Rack kann kippen und schwere Verletzungen verursachen.
  - Installationsanweisungen lesen, bevor das Rack in die Installationsposition gebracht wird.
  - Keine Gegenstände auf das auf den Schienen montierte Gerät in der Installationsposition legen.
  - Auf den Schienen montiertes Gerät nicht in der Installationsposition lassen.
- Ein Rackschrank kann mit mehreren Netzkabeln ausgestattet sein.
  - Wird bei Racks mit Wechselstrom während der Wartung dazu aufgefordert, den Rackschrank von der Stromversorgung zu trennen, müssen alle Netzkabel vom Rackschrank abgezogen werden.
  - Bei Racks mit einem Gleichstromverteiler den Sicherungsautomaten ausschalten, über den die Stromversorgung der Systemeinheit(en) gesteuert wird, oder die Verbindung zur Gleichstromquelle des Kunden trennen, wenn dazu aufgefordert wird, die Stromversorgung während der Wartung zu trennen.
- Alle in einem Rackschrank installierten Einheiten an Stromversorgungseinheiten anschließen, die in diesem Rackschrank installiert sind. Das Netzkabel einer in einen Rackschrank installierten Einheit nicht an eine Stromversorgungseinheit anschließen, die in einem anderen Rackschrank installiert ist.
- Bei nicht ordnungsgemäß angeschlossener Netzsteckdose können an Metallteilen des Systems oder an angeschlossenen Einheiten gefährliche Berührungsspannungen auftreten. Für den ordnungsgemäßen Zustand der Steckdose ist der Betreiber verantwortlich. (R001 Teil 1 von 2)

(R001 Teil 2 von 2):

Vorsicht:

- Eine Einheit nicht in einem Rack installieren, in dem die interne Temperatur der umgebenden Luft die vom Hersteller empfohlene Temperatur der umgebenden Luft für alle im Rack installierten Einheiten übersteigt.
- Eine Einheit nicht in einem Rack installieren, dessen Luftzirkulation beeinträchtigt ist. Die Lüftungsschlitze der Einheit dürfen nicht blockiert sein.
- Die Geräte müssen so an den Stromkreis angeschlossen werden, dass eine Überlastung der Stromkreise die Stromkreisverkabelung oder den Überstromschutz nicht beeinträchtigt. Damit ein ordnungsgemäßer Anschluss des Racks an den Stromkreis gewährleistet ist, anhand der auf den Einheiten im Rack befindlichen Typenschilder die Gesamtanschlusswerte des Stromkreises ermitteln.
- *Bei beweglichen Einschüben:* Keine Einschübe oder Einrichtungen herausziehen oder installieren, wenn am Rack kein Stabilisator befestigt ist oder wenn das Rack nicht am Boden verschraubt ist. Wegen Kippgefahr immer nur einen Einschub herausziehen. Werden mehrere Einschübe gleichzeitig herausgezogen, kann das Rack kippen.

- *Bei fest installierten Einschüben:* Fest installierte Einschübe dürfen bei einer Wartung nur dann herausgezogen werden, wenn dies vom Hersteller angegeben wird. Wird versucht, den Einschub ganz oder teilweise aus seiner Installationsposition im Gestell herauszuziehen, kann das Gestell kippen oder der Einschub aus dem Rack herausfallen. (R001 Teil 2 von 2)

Vorsicht: Werden während des Standortwechsels Komponenten aus den oberen Positionen des Rackschranks ausgebaut, verbessert sich die Rackstabilität. Die folgenden allgemeinen Richtlinien beachten, wenn ein gefüllter Rackschrank innerhalb eines Raumes oder Gebäudes an einen anderen Standort gebracht wird.

- Das Gewicht des Rackschranks reduzieren, indem Geräte von oben nach unten aus dem Rackschrank ausgebaut werden. Nach Möglichkeit die Konfiguration wiederherstellen, die der Rackschrank bei der Lieferung hatte. Ist diese Konfiguration nicht bekannt, müssen die folgenden Vorsichtsmaßnahmen beachtet werden:
  - Alle Einheiten in der Position HE 32 und höheren Positionen entfernen.
  - Darauf achten, dass die schwersten Einheiten unten im Rackschrank installiert sind.
  - Darauf achten, dass im Rackschrank zwischen den unter Position 32U installierten Einheiten keine oder ganz wenige U-Positionen leer sind, wenn dies in der erhaltenen Konfiguration nicht ausdrücklich zugelassen wird.
- Sind mehrere Rackschränke miteinander verbunden, sollten diese vor einem Positionswechsel getrennt und einzeln umgezogen werden.
- Wurde der für den Standortwechsel vorgesehene Rackschrank mit ausbaubaren Auslegern geliefert, müssen diese Ausleger wieder angebracht werden, bevor der Schrank transportiert wird.
- Den vorgesehenen Transportweg überprüfen, um mögliche Gefahrenquellen zu eliminieren.
- Überprüfen, ob der Boden auf dem gesamten Transportweg das Gewicht des voll bestückten Rackschranks tragen kann. Informationen über das Gewicht eines voll bestückten Rackschranks enthält die mit dem Rackschrank gelieferte Dokumentation.
- Überprüfen, ob alle Klappen mindestens 76 cm breit und 208,3 cm hoch sind.
- Überprüfen, ob alle Einheiten, Fächer, Einschübe, Türen und Kabel sicher befestigt sind.
- Überprüfen, ob die vier Ausgleichsunterlagen auf der höchsten Position stehen.
- Darauf achten, dass während des Transports keine Stabilisatoren am Rackschrank angebracht sind.
- Keine Rampen mit einer Neigung von mehr als zehn Grad benutzen.
- Befindet sich der Rackschrank an dem neuen Standort, die folgenden Schritte ausführen:
  - Die vier Ausgleichsunterlagen absenken.
  - Stabilisatoren am Rackschrank anbringen oder in einer erdbebengefährdeten Umgebung das Rack am Boden verschrauben.

– Wurden Einheiten aus dem Rackschrank ausgebaut, den Rackschrank von unten nach oben wieder bestücken.

- Erfolgt der Standortwechsel über eine größere Entfernung, die Konfiguration wiederherstellen, die der Rackschrank bei der Lieferung hatte. Den Rackschrank in die Originalverpackung oder eine gleichwertige Verpackung einpacken. Zudem die Ausgleichsunterlagen so absenken, dass sich die Gleitrollen von der Palette abheben. Dann den Rackschrank mit Bolzen an der Palette befestigen.

(R002)

(L001)

Gefahr: In Komponenten, die diesen Aufkleber aufweisen, treten gefährliche Spannungen, Ströme oder Energien auf. Keine Abdeckungen oder Sperren öffnen, die diesen Aufkleber aufweisen. (L001)

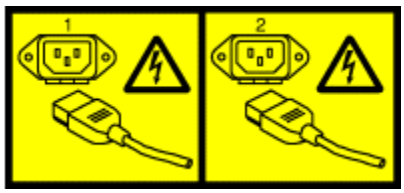
(L002)

Gefahr: In einem Rack installierte Einheiten dürfen nicht als Tische oder Ablagen missbraucht werden. Keine Gegenstände auf die in einem Rack installierten Einheiten legen. Außerdem nicht an in einem Rack installierte Einheiten anlehnen und diese Einheiten nicht zur Stabilisierung Ihrer Position verwenden (z. B. bei der Arbeit auf einer Leiter). Gefahr bezüglich Stabilität:

- Das Rack kann kippen und schwere Verletzungen verursachen.
- Installationsanweisungen lesen, bevor das Rack in die Installationsposition gebracht wird.
- Keine Gegenstände auf das auf den Schienen montierte Gerät in der Installationsposition legen.
- Auf den Schienen montiertes Gerät nicht in der Installationsposition lassen.

(L002)

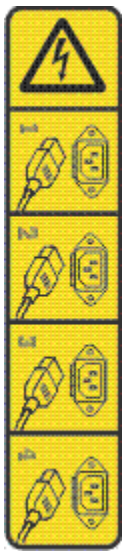
(L003)



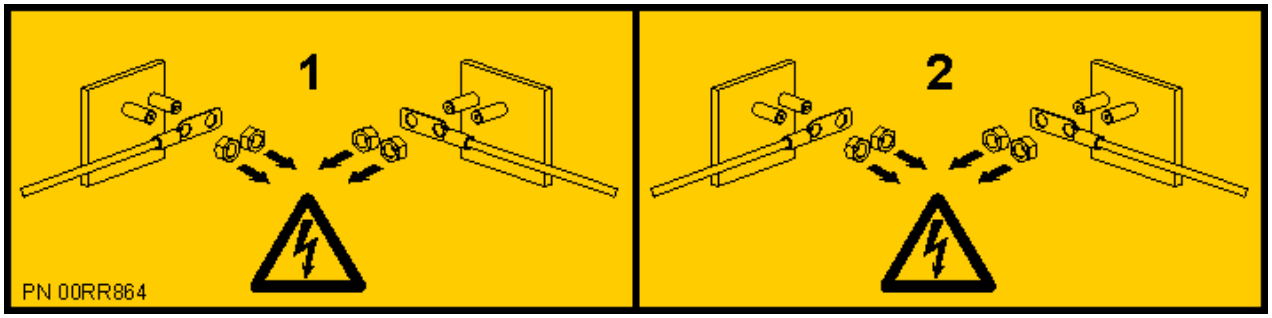
oder

oder

oder



oder



Gefahr: Mehrere Netzkabel. Dieses Produkt kann mit mehreren Wechselstromkabeln oder mehreren Gleichstromkabeln ausgestattet sein. Alle Netzkabel abziehen, um gefährliche Spannungen zu verhindern. (L003)

(L007)

Vorsicht: Heiße Oberfläche in der Nähe. (L007)

(L008)

Vorsicht: Gefährliche bewegliche Teile in der Nähe. (L008)

Alle Laser entsprechen den Normen IEC 60825 und EN 60825 für Laserprodukte der Klasse 1. Die Etiketten auf den einzelnen Teilen enthalten die Laserzertifizierungsnummern und die zugehörige Lasernorm.

Vorsicht: Dieses Produkt kann ein CD-ROM-Laufwerk, ein DVD-ROM-Laufwerk, ein DVD-RAM-Laufwerk und/oder ein Lasermodul mit einem Laser der Klasse 1 enthalten. Folgendes beachten:

- Die Abdeckungen nicht ausbauen. Durch Ausbauen der Abdeckungen der Lasergeräte können gefährliche Laserstrahlungen freigesetzt werden. Die Einheit enthält keine zu wartenden Teile.
- Werden Steuerelemente, Einstellungen oder Prozeduren anders als hier angegeben verwendet, kann gefährliche Laserstrahlung auftreten.

(C026)

Vorsicht: In Datenverarbeitungsumgebungen können Geräte eingesetzt werden, die Systemleitungen mit Lasermodulen verwenden, die die Werte der Klasse 1 überschreiten. Aus diesem Grund nie in das offene Ende eines Glasfaserkabels oder einer offenen Anschlussbuchse schauen. Wird die Leitfähigkeit eines Glasfaserkabels geprüft, indem in ein Ende eines nicht angeschlossenen Glasfaserkabels hineingeleuchtet und in das andere Ende hineingeschaut wird, ist zwar grundsätzlich keine Schädigung des Auges zu erwarten, dennoch ist diese Vorgehensweise potenziell gefährlich. Es wird daher davon abgeraten, die Leitfähigkeit des Glasfaserkabels zu prüfen, indem auf der einen Seite hineingeleuchtet und auf der anderen Seite hineingeschaut wird. Um die Leitfähigkeit eines Glasfaserkabels zu prüfen, eine optische Lichtquelle und ein Messgerät verwenden. (C027)

Vorsicht: Dieses Produkt enthält einen Laser der Klasse 1. Niemals direkt mit optischen Instrumenten in den Laserstrahl blicken. (C028)

Vorsicht: Einige Lasergeräte enthalten eine Laserdiode der Klasse 3A oder 3B. Folgendes beachten:

- Laserstrahlung bei geöffneter Verkleidung.
- Nicht in den Strahl blicken. Keine Lupen oder Spiegel verwenden. Strahlungsbereich meiden. (C030)

(C030)

Vorsicht: Die Batterie enthält Lithium. Die Batterie nicht verbrennen oder aufladen.

Die Batterie nicht:

- mit Wasser in Berührung bringen.
- Über 100 Grad Celsius erhitzen.
- reparieren oder zerlegen.

Nur gegen das von IBM Teil austauschen. Batterie nach Gebrauch der Wiederverwertung zuführen oder als Sondermüll entsorgen. IBM Deutschland beteiligt sich am Gemeinsamen Rücknahme System GRS für Batterien (www.grs-batterien.de). Die Batterien müssen in den Behältern des GRS entsorgt werden, die an allen Verkaufsstellen zur Verfügung stehen. Alternativ können sie auch an das Rücknahmezentrum Mainz geschickt werden (www.ibm.com/de/umwelt/ruecknahme). (C003)

Vorsicht: Bei der Verwendung eines von IBM bereitgestellten Hebewerkzeugs:

- Das Hebewerkzeug darf nur von autorisiertem Personal verwendet werden.
- Das Hebewerkzeug dient ausschließlich als Hilfe zum Anheben beim Ein- und Ausbau von Einheiten in einem Rack. Es darf nicht zum Transport über größere Rampen oder als Ersatz für Palettenheber, Gabelstapler und ähnliche Geräte verwendet werden. Wenn dies nicht möglich ist, müssen entsprechend geschulte Fachleute oder Services (z. B. Monteure oder Umzugsfirmen) die Einheit installieren.
- Die Anweisungen für das Hebewerkzeug vor dem Gebrauch sorgfältig durchlesen. Werden Sicherheitsregeln und Anweisungen nicht beachtet, können Verletzungen und/oder Schäden an Geräten auftreten. Wenden Sie sich bei Fragen an den Service und Support des Herstellers des Hebewerkzeugs. Das mitgelieferte Handbuch muss nach dem Gebrauch wieder in die dafür vorgesehene Hülle zurückgelegt werden. Auf der Website des Herstellers ist die neueste Version des Handbuchs verfügbar.
- Vor jedem Gebrauch die Funktion der Stabilisatorbremse überprüfen. Nicht versuchen, das Hebewerkzeug bei angezogener Stabilisatorbremse zu heftig zu bewegen oder zu rollen.
- Das Anheben, Absenken oder Verschieben der Plattform darf nur bei vollständig eingerastetem Stabilisator (Bremspedal) erfolgen. Ist das Hebewerkzeug nicht im Gebrauch, die Stabilisatorbremse eingerastet lassen.
- Das Hebewerkzeug bei angehobener Plattform nur minimal bewegen.
- Das Hebewerkzeug nicht über die angegebene Nennlastkapazität hinaus beladen. Informationen zur maximalen Last in der Mitte und am Rand der ausgefahrenen Plattform enthält die Lastkapazitätstabelle.
- Die Last nur anheben, wenn sie mittig auf der Plattform platziert ist. Nicht mehr als 91 kg Last am Rand der beweglichen Plattform platzieren. Dabei auch den Schwerpunkt der Last beachten.
- Den Rand der Plattformen, der Vorrichtung zur Schrägstellung, des Keils für die Installation der Winkeleinheit oder anderer Zubehöroptionen nicht beladen. Solche Plattformen (Vorrichtung zur Schrägstellung, Keil usw.) vor der Verwendung ausschließlich mit der bereitgestellten Hardware an allen vier Positionen (vier Positionen oder allen anderen bereitgestellten Montagepositionen) der Ablage oder der Verzweigungen der Haupthebevorrichtung befestigen. Ladeobjekte lassen sich ohne größeren Kraftaufwand auf glatten Plattformen bewegen. Daher ein unabsichtliches

Bewegen der Last vermeiden. Die Vorrichtung zur Schrägstellung [Plattform für konfigurierbare Winkel] außer bei erforderlichen kleinen Winkelkorrekturen immer in der flachen Position lassen.

- Nicht unter überhängende Lasten stellen.
- Keine unebene Oberfläche und keine Steigungen oder Gefälle (größere Rampen) verwenden.
- Keine Lasten stapeln.
- Das Hebewerkzeug nicht unter Einfluss von Medikamenten oder Alkohol bedienen.
- Die Leiter nicht an das HEBEWERKZEUG anlehnen (es sei denn, dies wird für eine der folgenden qualifizierten Prozeduren bei der Arbeit mit diesem HEBEWERKZEUG zugelassen).
- Kippgefahr. Bei angehobener Plattform nicht gegen die Last drücken.
- Die Plattform nicht zum Anheben oder Transportieren von Personen und nicht als Trittbrett verwenden.
- Das Hebewerkzeug nicht betreten. Das Hebewerkzeug nicht als Trittbrett verwenden.
- Nicht auf den Mast klettern.
- Ein beschädigtes oder nicht ordnungsgemäß funktionierendes Hebewerkzeug nicht verwenden.
- Einklemm- oder Quetschgefahr unter der Plattform. Last nur in Bereichen ohne Personen und Hindernisse absenken. Hände und Füße beim Betrieb vom Hebewerkzeug fernhalten.
- Keine Gabeln. Das Hebewerkzeug nicht mit einem Palettenwagen, Palettenheber oder Gabelstapler anheben oder bewegen.
- Der Mast ist höher als die Plattform. Auf die Deckenhöhe, auf Kabelfächer, Sprinkler, Lichtquellen und andere Objekte über Kopfhöhe achten.
- Hebewerkzeug bei angehobener Plattform nicht unbeaufsichtigt lassen.
- Darauf achten, dass Hände, Finger und Kleidung nicht mit beweglichen Teilen in Berührung kommen.
- Winde nur mit der Hand drehen. Kann der Griff der Winde nicht leicht mit einer Hand gedreht werden, ist das Hebewerkzeug möglicherweise überladen. Die Winde nicht über den oberen und unteren Funktionsbereich der Plattform hinaus drehen. Bei einem zu starken Abspulen löst sich der Griff und wird das Kabel beschädigt. Beim Absenken der Plattform den Griff der Winde immer festhalten. Vor dem Loslassen des Griffs der Winde immer sicherstellen, dass die Winde die Last hält.
- Bei einem durch die Winde verursachten Unfall können schwere Verletzungen auftreten. Keine Personen transportieren. Beim Anheben des Geräts muss ein Klicken hörbar sein. Vor dem Loslassen des Griffs sicherstellen, dass die Winde gesperrt ist. Vor dem Betrieb der Winde die Seite mit den Anweisungen lesen. Darauf achten, dass sich die Winde nie frei abspult. Das freie Abspulen kann zu einem unebenen Umlauf des Kabels um die Windentrommel und zu einer Beschädigung des Kabels und zu schweren Verletzungen führen.
- Dieses WERKZEUG muss für die Verwendung durch IBM Service-Personal ordnungsgemäß gewartet werden. IBM untersucht vor dem Betrieb den Zustand und überprüft den Wartungsverlauf. Das Personal behält sich das Recht vor, das WERKZEUG bei Unzulänglichkeit nicht zu verwenden. (C048)

Stromversorgungs- und Verkabelungsinformationen, die dem Standard für elektromagnetische Verträglichkeit und elektrische Sicherheit GR-1089-CORE entsprechen

Die folgenden Kommentare beziehen sich auf die IBM Server, die dem Standard für elektromagnetische Verträglichkeit und elektrische Sicherheit GR-1089-CORE entsprechen.

Diese Geräte sind für die Installation in folgenden Bereichen geeignet:

- Netz-Telekommunikationseinrichtungen
- Standorte, die den Normen des jeweiligen Landes entsprechen müssen

Die Anschlüsse dieses Geräts sind nur für Verbindungen zu im Gebäude liegenden oder nicht der Außenumgebung ausgesetzten Kabeln geeignet. Die Anschlüsse dieses Geräts dürfen keine elektrische Verbin-

dung zu Schnittstellen haben, die an eine Anlage oder deren Verkabelung angeschlossen sind, welche das Gebäude verlässt (Outside Plant OSP). Diese Schnittstellen wurden nur für die Verwendung innerhalb geschlossener Gebäude entwickelt (Anschlüsse vom Typ 2 oder Typ 4, wie im Standard für elektromagnetische Verträglichkeit und elektrische Sicherheit GR-1089-CORE beschrieben). Hierbei ist eine Isolierung der gebäudeinternen Verkabelung zur Verkabelung außerhalb des Gebäudes erforderlich. Das Hinzufügen von primären Schutzvorrichtungen stellt keinen ausreichenden Schutz dar, wenn diese Schnittstellen eine elektrische Verbindung zu der Verkabelung haben, die das Gebäude verlässt.

Anmerkung: Alle Ethernet-Kabel müssen an beiden Enden abgeschirmt und geerdet sein.

Für das Wechselstromsystem ist keine externe Überspannungsschutzeinheit erforderlich.

Das Gleichstromsystem benutzt ein Design mit isolierter Gleichstromrückleitung (DC-I). Der Gleichstrom-Rückleitungsanschluss der Batterie darf *nicht* an das Chassis oder die Rahmenerdung angeschlossen werden.

Das Gleichstromsystem ist für die Installation in einem Common Bonding Network (CBN) vorgesehen, wie im Standard für elektromagnetische Verträglichkeit und elektrische Sicherheit GR-1089-CORE beschrieben.

Hardware Management Console installieren und konfigurieren

In diesem Abschnitt wird beschrieben, wie die Hardware Management Console (HMC) installiert, an das verwaltete System angeschlossen und zur Verwendung konfiguriert wird. Sie können diese Aufgaben selbst ausführen oder einen Service-Provider damit beauftragen. Dieser Service ist möglicherweise nicht kostenlos.

Neuerungen bei diesem Handbuch

Hier erfahren Sie, welche neuen oder signifikant geänderten Informationen im Thema "Hardware Management Console - Installation und Konfiguration" seit der letzten Aktualisierung der Themensammlung dazugekommen sind.

April 2021

- Folgende Abschnitte wurden hinzugefügt:
  - „IBM Power Systems HMC (7063-CR2) in einem Rack installieren” auf Seite 4
  - „Voraussetzungen für die Installation des Einschubsystems vom Typ 7063-CR2” auf Seite 4
  - „Bestandsaufnahme für Ihr System ausführen” auf Seite 5
  - „Position im Rack für das System vom Typ 7063-CR2 bestimmen und markieren” auf Seite 5
  - „Verstellbare Schienen am Systemchassis und am Rack anbringen” auf Seite 7
  - „Fixierte Schienen am Systemchassis und am Rack anbringen” auf Seite 9
  - „System im Rack installieren und Netzkabel anschließen und verlegen” auf Seite 10
  - „In einem Rack installierte HMC 7063-CR2 verkabeln” auf Seite 11
  - „HMC 7063-CR2 konfigurieren” auf Seite 12

November 2020

- Folgende Abschnitte aktualisiert:
  - „Installations- und Konfigurationstasks” auf Seite 2
  - „HMC sichern” auf Seite 90
  - „HMC-Anschlusspositionen” auf Seite 98

Juli 2020

- Folgende Abschnitte aktualisiert:
  - „Virtuelle HMC-Appliance installieren ” auf Seite 25
  - „HMC-Anschlusspositionen” auf Seite 98

Oktober 2019

- Folgende Abschnitte aktualisiert:
  - „Virtuelle HMC-Appliance installieren ” auf Seite 25
  - „HMC sichern” auf Seite 90

Februar 2019

- Folgende Abschnitte wurden hinzugefügt:
  - „HMC sichern" auf Seite 90
  - „Erweiterte Kennwortrichtlinie" auf Seite 92
  - „Allgemeine Probleme beim Sichern der HMC beheben" auf Seite 95
  - „Sicherheitsprofile: Datenschutzgrundverordnung (DSGVO) und Payment Card Industry Data Security Standard (PCI-DSS) " auf Seite 94

August 2018

- Folgende Abschnitte aktualisiert:
  - „HMC 7063-CR1 konfigurieren" auf Seite 22
  - „HMC-Anschlusspositionen" auf Seite 98

Dezember 2017

- Informationen zu IBM Power Systems-Servern mit POWER9-Prozessor hinzugefügt.

Installations- und Konfigurationstasks

Hier erfahren Sie mehr über die verschiedenen Installations- und Konfigurationstasks der HMC.

Dieser Abschnitt enthält eine ausführliche Beschreibung der Tasks, die Sie bei der Installation und Konfiguration der HMC ausführen müssen. Die HMC kann mit verschiedenen Methoden installiert und konfiguriert werden. Suchen Sie die Situation, die der Task, die Sie ausführen möchten, am ehesten entspricht.

Notes:

- Wenn Sie Server mit POWER9-Prozessor verwalten, müssen Sie eine HMC ab Version 9.1.0 verwenden. Weitere Informationen finden Sie unter „Version und Release Ihres HMC-Maschinencodes bestimmen" auf Seite 79.
- Hardware Management Console ab Version 9.2.950 wird für den Maschinentyp HMC 7042 nicht unterstützt. Weitere Informationen zu den HMC-Versionen für Ihre HMC 7042 finden Sie in den HMC-Releaseinformationen, die auf der Fix Central-Website verfügbar sind.

Neue HMC mit einem neuen Server installieren und konfigurieren

Hier erfahren Sie mehr über die generellen Tasks, die Sie ausführen müssen, wenn Sie eine neue HMC mit einem neuen Server installieren und konfigurieren.

Tabelle 1. Erforderliche Tasks bei der Installation und Konfiguration einer neuen HMC mit einem neuen Server

Task	Referenzinformationen
1. Stellen Sie Informationen zusammen und gehen Sie das Preinstallation Configuration Worksheet (Arbeitsblatt zur Konfiguration bei der Installationsvorbereitung) durch.	„Arbeitsblatt zur Konfiguration bei der Installationsvorbereitung für die HMC" auf Seite 49 „HMC-Konfiguration vorbereiten" auf Seite 48
2. Entpacken Sie die Hardware.	
3. Verkabeln Sie die HMC-Hardware.	„In einem Rack installierte HMC 7063-CR1 verkabeln" auf Seite 20
4. Drücken Sie den Netzschalter, um die HMC einzuschalten.	

Tabelle 1. Erforderliche Tasks bei der Installation und Konfiguration einer neuen HMC mit einem neuen Server (Forts.)	
Task	**Referenzinformationen**
5. Melden Sie sich an und starten Sie die HMC-Webanwendung.	
6. Greifen Sie auf den Guided Setup Wizard zu oder verwenden Sie die HMC-Menüs für die Konfiguration der HMC.	„HMC mithilfe des Direktaufrufs durch den Guided Setup Wizard konfigurieren” auf Seite 57 „HMC mithilfe der Menüs konfigurieren ” auf Seite 57
7. Schließen Sie den Server an die HMC an.	

HMC-Code aktualisieren und Upgrade durchführen

Hier erfahren Sie mehr über die generellen Tasks, die Sie ausführen müssen, wenn Sie den HMC-Code aktualisieren und ein Upgrade durchführen.

Wenn eine HMC vorhanden ist und Sie den HMC-Code aktualisieren bzw. ein Upgrade durchführen möchten, müssen Sie die folgenden generellen Tasks ausführen:

Tabelle 2. Erforderliche Tasks bei Aktualisierung oder Upgrade von HMC-Code	
Task	**Referenzinformationen**
1. Upgrade besorgen	„Upgrade der HMC-Software durchführen” auf Seite 85
2. Vorhandene HMC-Maschinencodeversion anzeigen	
3. Profildaten des verwalteten Systems sichern	
4. HMC-Daten sichern	
5. Aktuelle HMC-Konfigurationsdaten notieren	
6. Status des fernen Befehls notieren	
7. Upgradedaten speichern	
8. Upgrade der HMC-Software durchführen	
9. Überprüfen, ob das Upgrade für den HMC-Maschinencode erfolgreich installiert wurde	

Eine zweite HMC einer bestehenden Installation hinzufügen

Hier erfahren Sie mehr über die generellen Tasks, die Sie ausführen müssen, wenn Sie eine zweite HMC dem verwalteten System hinzufügen.

Wenn eine HMC und ein verwaltetes System vorhanden sind und Sie dieser Konfiguration eine zweite HMC hinzufügen möchten, führen Sie die folgenden Schritte aus:

Tabelle 3. Erforderliche Tasks beim Hinzufügen einer zweiten HMC zu einer bestehenden Installation	
Task	**Referenzinformationen**
1. Stellen Sie sicher, dass die HMC-Hardware den Code von einer HMC Version 7 unterstützt.	

Tabelle 3. Erforderliche Tasks beim Hinzufügen einer zweiten HMC zu einer bestehenden Installation (Forts.)	
Task	**Referenzinformationen**
2. Stellen Sie Informationen zusammen und gehen Sie das Preinstallation Configuration Worksheet (Arbeitsblatt zur Konfiguration bei der Installationsvorbereitung) durch.	„Arbeitsblatt zur Konfiguration bei der Installationsvorbereitung für die HMC" auf Seite 49
3. Entpacken Sie die Hardware.	
4. Verkabeln Sie die HMC-Hardware.	„In einem Rack installierte HMC 7063-CR1 verkabeln" auf Seite 20
5. Drücken Sie den Netzschalter, um die HMC einzuschalten.	
6. Melden Sie sich an der HMC an.	
7. Die Versionen des HMC-Codes müssen übereinstimmen. Ändern Sie den Code auf einer der HMCs, damit dieser mit dem Code der anderen übereinstimmt.	„Version und Release Ihres HMC-Maschinencodes bestimmen" auf Seite 79 „Upgrade der HMC-Software durchführen" auf Seite 85
8. Greifen Sie auf den Guided Setup Wizard zu oder verwenden Sie die HMC-Menüs für die Konfiguration der HMC.	„HMC mithilfe der Menüs konfigurieren " auf Seite 57
9. Konfigurieren Sie diese HMC für Service unter Verwendung des Installationsassistenten für die Call-Home-Funktion.	„HMC für die Verbindung zu Service und Support unter Verwendung des Installationsassistenten für die Call-Home-Funktion konfigurieren" auf Seite 72
10. Schließen Sie den Server an die HMC an.	

HMC installieren

Sie müssen zunächst die HMC-Hardware installieren, bevor Sie die HMC-Software konfigurieren. Im Folgenden erhalten Sie weitere Informationen über die Installation einer HMC in einem Deskside-System oder in einem Rack.

IBM Power Systems HMC (7063-CR2) in einem Rack installieren

Hier erfahren Sie, wie Sie die IBM Power Systems HMC (7063-CR2) in einem Rack installieren.

Sie können die Installationsdokumentation online anzeigen oder die PDF-Version mit denselben Informationen drucken. Informationen zum Anzeigen oder Drucken der PDF-Version finden Sie unter Hardware Management Console installieren und konfigurieren.

Voraussetzungen für die Installation des Einschubsystems vom Typ 7063-CR2

Hier finden Sie Informationen zu den Voraussetzungen, die für die Installation des Systems erforderlich sind.

Informationen zu diesem Vorgang

Vorsicht: Dieses Teil oder diese Einheit ist schwer, wiegt jedoch weniger als 18 kg. Beim Anheben, Ausbauen oder Installieren dieses Teils oder dieser Einheit vorsichtig vorgehen. (C008)

Bevor Sie mit der Installation des Servers beginnen, sollten Sie die folgenden Dokumente lesen:

- Die aktuelle Version dieses Dokuments wird online verwaltet. Siehe 7063-CR2 in einem Rack installieren (http://www.ibm.com/support/knowledgecenter/POWER9/p9hai/p9hai_install7063cr2_kickoff.htm).
- Informationen zur Planung Ihrer Serverinstallation finden Sie unter Standort- und Hardwareplanung.

Vorgehensweise

1. Vergewissern Sie sich, dass Sie vor Beginn der Installation Folgendes zur Hand haben:
   - Kreuzschlitz-Schraubendreher der Größe 2
   - Schlitzschraubendreher
   - T25-Schraubendreher
   - Teppichmesser
   - Antistatikarmband zum Schutz vor elektrostatischer Entladung
   - Rack mit einer freien EIA-Einheit (1U)

   Notes:

   - Ist kein Rack installiert, installieren Sie das Rack. Entsprechende Anweisungen finden Sie unter Racks und Rack-Features (http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_9xx_kickoff.htm).
   - Die Nennstromstärke der Netzteile beträgt 100 bis 127 V Wechselspannung, 9 A (x2), 200 bis 240 V Wechselspannung, 4,5 A (x2); 50 oder 60 Hertz.
2. Fahren Sie mit „Bestandsaufnahme für Ihr System ausführen” auf Seite 5 fort.

Bestandsaufnahme für Ihr System ausführen

Verwenden Sie diese Informationen, um eine Bestandsaufnahme für Ihr System auszuführen.

Vorgehensweise

1. Überprüfen Sie, ob Sie alle bestellten Pakete erhalten haben.
2. Packen Sie die Serverkomponenten aus.
3. Führen Sie vor der Installation jeder Serverkomponente eine Bestandsaufnahme durch und überprüfen Sie, ob Sie alle bestellten Teile erhalten haben.

   Anmerkung:

   Die Bestellinformationen sind Teil des Produkts. Bestellinformationen können Sie auch über den Vertriebsbeauftragten oder den IBM Business Partner erhalten.

   Ist die Lieferung falsch, fehlen Teile oder sind Teile beschädigt, wenden Sie sich an eine der folgenden Stellen:

   - IBM Reseller.
   - In den USA unter der Telefonnummer 1-800-300-8751 an die IBM Rochester Manufacturing Automated Information Line.
   - Website mit dem Verzeichnis der weltweiten Kontakte (http://www.ibm.com/planetwide). Wählen Sie Ihren Standort aus, um die Kontaktinformationen für Service und Support aufzurufen.
4. Fahren Sie mit „Position im Rack für das System vom Typ 7063-CR2 bestimmen und markieren” auf Seite 5 fort.

Position im Rack für das System vom Typ 7063-CR2 bestimmen und markieren

Sie müssen die Position bestimmen, an der die Systemeinheit im Rack installiert werden soll.

Vorgehensweise

1. Lesen Sie die Racksicherheitshinweise (http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_racksafety.htm).
2. Ermitteln Sie, wo die Systemeinheit im Rack angeordnet werden soll. Berücksichtigen Sie bei der Planung der Installation der Systemeinheit in einem Rack die folgenden Informationen:
   - Ordnen Sie große und schwere Einheiten im unteren Bereich des Racks an.
   - Planen Sie, Systemeinheiten zunächst im unteren Bereich des Racks zu installieren.
   - Erfassen Sie die EIA-Positionen (EIA = Electronic Industries Alliance) in Ihrem Plan.
3. Falls erforderlich, bauen Sie die Abdeckblenden aus, um auf die Positionen im Inneren des Rackschranks zugreifen zu können, an denen die Einheiten installiert werden sollen, wie in Abbildung 1 auf Seite 6 dargestellt.

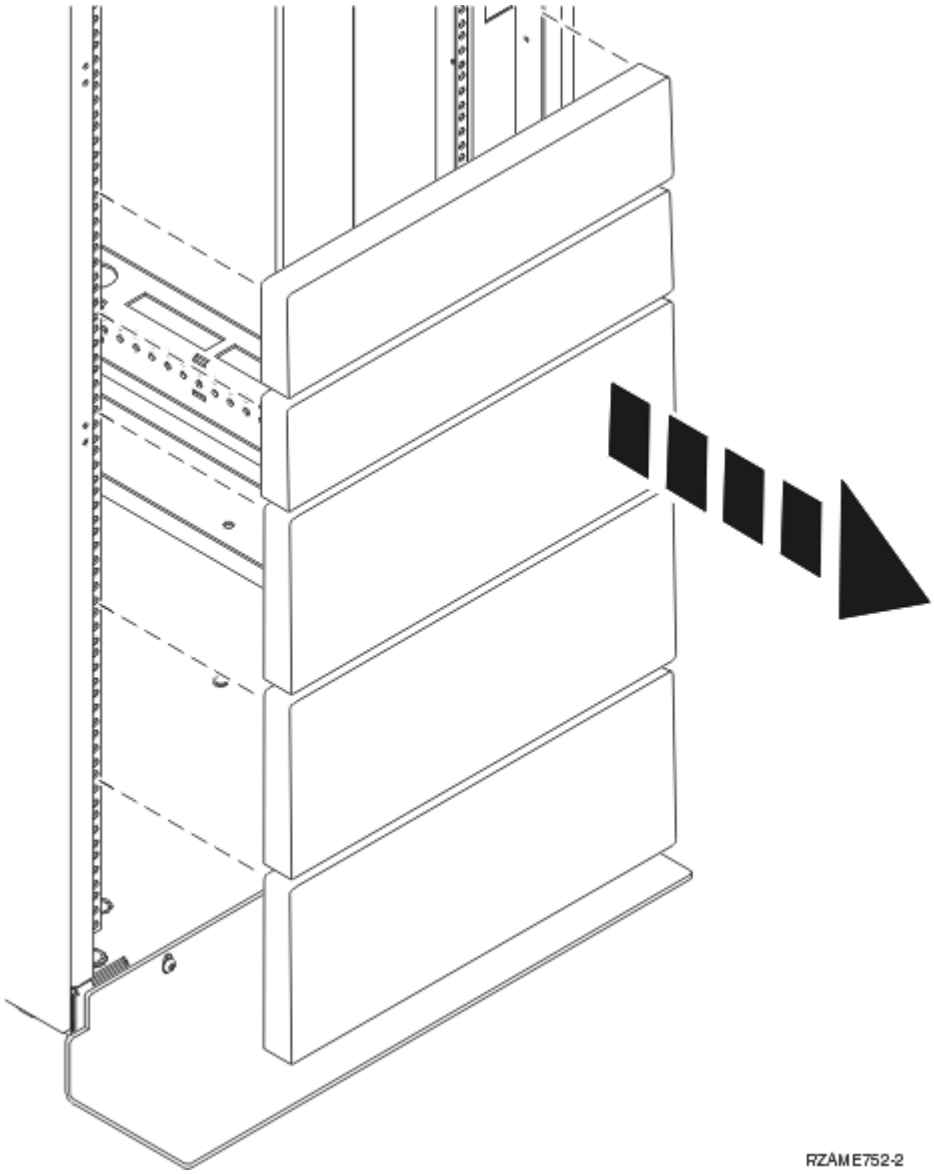


Abbildung 1. Abdeckblenden ausbauen

4. Bestimmen Sie die Position des Systems im Rack. Notieren Sie die EIA-Position.
5. Stellen Sie sich vor die Vorderseite des Racks und markieren Sie auf der rechten Seite mithilfe eines Bandes, eines Markers oder eines Stiftes die niedrigere Bohrung der einzelnen EIA-Einheiten.
6. Wiederholen Sie Schritt „5” auf Seite 6 für die entsprechenden Löcher auf der linken Seite des Racks.
7. Gehen Sie an die Rückseite des Racks.

8. Suchen Sie auf der rechten Seite die EIA-Einheit, die der auf der Vorderseite des Racks gekennzeichneten unteren EIA-Einheit entspricht.
9. Markieren Sie die untere EIA-Einheit.
10. Markieren Sie die entsprechenden Löcher auf der linken Seite des Racks.
11. Fahren Sie mit „Verstellbare Schienen am Systemchassis und am Rack anbringen” auf Seite 7 fort, um die verstellbaren Schienen anzubringen, oder mit „Fixierte Schienen am Systemchassis und am Rack anbringen” auf Seite 9, um die befestigten Schienen anzubringen.

Verstellbare Schienen am Systemchassis und am Rack anbringen

Sie müssen die Schienen auf dem Chassis und am Rack installieren. Verwenden Sie für diese Aufgabe das folgende Verfahren.

Informationen zu diesem Vorgang

Achtung: Um Fehler an der Schienenführung und mögliche Gefahren für Sie und die Einheit zu vermeiden, muss darauf geachtet werden, dass die korrekten Schienen und Verbindungsstücke für das Rack benutzt werden. Die Schienen im Rack haben quadratische oder runde Flanschbohrungen. Achten Sie darauf, dass die Schienen und Verbindungsstücke den Flanschbohrungen im Rack entsprechen. Bei nicht passenden Teilen keine Unterlegscheiben oder Abstandshalter verwenden. Sind die korrekten Schienen und Verbindungsstücke für das Rack nicht vorhanden, wenden Sie sich an Ihren IBM Reseller.

Anmerkung: 1 EIA-Einheit in Racks wird in vertikalen Schritten von je 44,45 mm (1,75 Zoll) gemessen. Jeder Schritt von 44,45 mm (1,75 Zoll) wird als “EIA” bezeichnet. In einigen Ländern kann der gleiche Schritt als “U” bezeichnet werden.

Anmerkung: Für das System ist 1 EIA-Rackeinheit (1U) an Platz erforderlich.

Stellen Sie sicher, dass Sie über alle Teile verfügen, die Sie für die Installation der Schienen benötigen. Folgende Teile sind im Schienensatz enthalten:

- 4 - Kreuzschlitzschrauben à 6,35 mm (0,25 Zoll)
- 2 - Baugruppen für Rack und Schienenhalterungen
- 2 - HMC-Schienenhalterungen
- 10 - Klemmmuttern für quadratische EIA-Bohrungen
- 10 - Klemmmuttern für runde EIA-Bohrungen
- 10 - Hexadezimale Flanschschrauben (M5)

Vorgehensweise

1. Nehmen Sie die Teile der Schienen aus der Verpackung und legen Sie sie auf eine Arbeitsoberfläche.
2. Ermitteln Sie 1 HE im Rack der HMC.
3. Führen Sie die folgenden Schritte aus, um die Schienenhalterungen an der HMC anzubringen:
   a. Ermitteln Sie die rechte Schienenhalterung.
   b. Richten Sie die Bohrlöcher an der rechten Schienenhalterung an den Stiften der Schienenhalterung aus, die sich auf der rechten Seite der HMC befinden. Stellen Sie sicher, dass die Stifte an den Halterungsbohrungen ausgerichtet sind.
   c. Schieben Sie die Schienenhalterung der HMC zur Rückseite der HMC, bis sie vollständig eingerastet ist.
   d. Befestigen Sie die rechte Schienenhalterung an der rechten Seite der HMC-Workstation, indem Sie zwei Kreuzschlitzschrauben à 6,35 cm (0,25 Zoll) in den Schraubenlöchern anbringen.
   e. Wiederholen Sie die Schritte „3.a” auf Seite 7 bis „3.d” auf Seite 7, um die linke Schienenhalterung an der linken Seite der HMC-Workstation zu installieren.
4. Gehen Sie zur Vorderseite des Racks.

a. Installieren Sie auf der linken Seite in den drei Bohrlöchern an der vorderen Kante des Racks im Steckplatz bei 1 HE, der für die HMC festgelegt ist, drei Klemmmuttern.

   Anmerkung: Der Schienensatz umfasst Klemmmuttern sowohl für quadratische als auch für runde Rackbohrungen. Stellen Sie sicher, dass Sie geeignete Klemmmuttern verwenden, die in die Bohrlöcher des Racks passen.

b. Wiederholen Sie Schritt „4.a" auf Seite 8 auf der rechten Seite des Racks.

5. Gehen Sie an die Rückseite des Racks.

   a. Installieren Sie auf der linken Seite im oberen und unteren Loch an der vorderen Kante des Racks im Steckplatz bei 1 HE, der für die HMC festgelegt ist, zwei Klemmmuttern.

      Anmerkung: Das mittlere Loch muss leer bleiben.

   b. Wiederholen Sie Schritt „5.a" auf Seite 8 auf der rechten Seite des Racks.

6. Führen Sie die folgenden Schritte aus, um die HMC-Schienen im Rack zu installieren:

   a. Messen Sie die Tiefe des Racks. Die Tiefe muss einen Wert zwischen 558,8 mm (22 Zoll) und 863,6 mm (34 Zoll) aufweisen.

   b. Legen Sie die HMC-Schienen auf eine flache Oberfläche und suchen Sie die vorinstallierten Schrauben.

      Anmerkung: Die Schienen weisen vier Schraubenlöcher auf.

   c. Lösen Sie die vorinstallierten Schrauben an den Schienen so weit, dass die Schienen ohne großen Aufwand rein- und rausgeschoben werden können.

   d. Basierend auf der in Schritt „6.a" auf Seite 8 gemessenen Tiefe des Racks müssen Sie die Schrauben an den Schienen anpassen.

      i) Beträgt die Tiefe des Racks zwischen 558,8 mm (22 Zoll) und 698,5 mm (27,5 Zoll), bringen Sie die Schrauben im ersten und dritten Loch an.

      ii) Beträgt die Tiefe des Racks zwischen 698,5 mm (27,5 Zoll) und 863,6 mm (34 Zoll), bringen Sie die Schrauben im zweiten und vierten Loch an.

      Notes:

      - Das erste Loch ist immer das am nächsten zum Ende der Schiene gelegene Loch. Das dritte und das vierte Loch liegen dicht beieinander.
      - Stellen Sie sicher, dass die Schrauben locker genug sind, damit die Länge der Schiene während der Installation im Rack leicht angepasst werden kann.

7. Führen Sie an der Vorderseite des Racks die folgenden Schritte aus, um die HMC-Schienen im Rack zu installieren:

   a. Suchen Sie die linke Schienenbaugruppe.

   b. Richten Sie die Schienenbaugruppe so aus, dass das Ende mit dem nächsten Schraubenloch (das erste Loch) zuerst in das Rack geht. Stellen Sie sicher, dass sich die Schraubenköpfe an der Innenseite des Racks befinden. Der offene Steckplatz der Schienenbaugruppe ist am nächsten zur Vorderseite des Racks gelegen.

   c. Befestigen Sie auf der linken Seite des Racks den Flansch mit zwei M5-Schrauben am Ende der Schiene an der vorderen Kante des Racks. In das mittlere Loch wird keine Schiene eingesetzt. Stellen Sie sicher, dass bei der Schienenbaugruppe an der Vorderseite des Racks etwas Spielraum gelassen wird, damit die HMC noch eingesetzt werden kann.

8. Ziehen Sie rechts an der Rückseite des Racks das freie Ende der Schiene zur Rückseite und befestigen Sie den Flansch der Schiene am Rack, indem Sie zwei M5-Schrauben anbringen. In das mittlere Loch wird keine Schraube eingesetzt.

9. Wiederholen Sie die Schritte „7" auf Seite 8 und „8" auf Seite 8, um die rechte Schienenbaugruppe an der rechten Seite des Racks zu installieren.

10. Führen Sie an der Vorderseite des Racks die folgenden Schritte aus, um die HMC-Workstation im Rack zu installieren:

a. Halten Sie den Hebel der HMC-Workstation und setzen Sie die Schienenhalterungen in die HMC-Schienen ein, die Sie im vorherigen Schritt installiert haben. Schieben Sie die HMC nach vorne, bis die Flansche an der Vorderseite der HMC bündig mit den offenen Schraubenlöchern anliegen, die sich an der Vorderseite des Racks befinden.

b. Befestigen Sie die HMC an der linken Seite des Rahmens mit einer M5-Schraube. Wiederholen Sie diesen Schritt auf der rechten Seite des Racks.

11. Fahren Sie mit „System im Rack installieren und Netzkabel anschließen und verlegen" auf Seite 10 fort.

Fixierte Schienen am Systemchassis und am Rack anbringen

Sie müssen die Schienen auf dem Chassis und am Rack installieren. Verwenden Sie für diese Aufgabe das folgende Verfahren.

Informationen zu diesem Vorgang

Achtung: Um Fehler an der Schienenführung und mögliche Gefahren für Sie und die Einheit zu vermeiden, muss darauf geachtet werden, dass die korrekten Schienen und Verbindungsstücke für das Rack benutzt werden. Die Schienen im Rack haben quadratische oder runde Flanschbohrungen. Achten Sie darauf, dass die Schienen und Verbindungsstücke den Flanschbohrungen im Rack entsprechen. Bei nicht passenden Teilen keine Unterlegscheiben oder Abstandshalter verwenden. Sind die korrekten Schienen und Verbindungsstücke für das Rack nicht vorhanden, wenden Sie sich an Ihren IBM Reseller.

Anmerkung: 1 EIA-Einheit in Racks wird in vertikalen Schritten von je 44,45 mm (1,75 Zoll) gemessen. Jeder Schritt von 44,45 mm (1,75 Zoll) wird als "EIA" bezeichnet. In einigen Ländern kann der gleiche Schritt als "U" bezeichnet werden.

Anmerkung: Für das System ist 1 EIA-Rackeinheit (1U) an Platz erforderlich.

Stellen Sie sicher, dass Sie über alle Teile verfügen, die Sie für die Installation der Schienen benötigen. Folgende Teile sind im Schienensatz enthalten:

- 4 - Kreuzschlitzschrauben à 6,35 mm (0,25 Zoll)
- 2 - Innere Schienen
- 2 - HMC-Trägerschienen
- 2 - Klemmmuttern für quadratische EIA-Bohrungen
- 2 - Klemmmuttern für runde EIA-Bohrungen
- 8 - Hexadezimale Flanschschrauben (M5)

Vorgehensweise

1. Nehmen Sie die Teile der Schienen aus der Verpackung und legen Sie sie auf eine Arbeitsoberfläche.
2. Ermitteln Sie 1 HE im Rack der HMC.
3. Führen Sie die folgenden Schritte aus, um die inneren Schienen an der HMC anzubringen:

   a. Ermitteln Sie die rechte innere Schiene.

   b. Richten Sie die Bohrungen an der rechten inneren Schiene an den inneren Schienenstiften aus, die sich auf der rechten Seite der HMC befinden. Stellen Sie sicher, dass die Stifte an den Bohrungen der inneren Schiene ausgerichtet sind.

   c. Schieben Sie die innere HMC-Schiene zur Vorderseite der HMC, bis sie vollständig eingerastet ist.

   d. Befestigen Sie die rechte innere Schiene an der rechten Seite der HMC-Workstation, indem Sie zwei Kreuzschlitzschrauben à 6,35 cm (0,25 Zoll) in den Schraubenlöchern anbringen.

   e. Wiederholen Sie die Schritte 3.a bis „3.d" auf Seite 9, um die linke innere Schiene an der linken Seite der HMC-Workstation zu installieren.

4. Gehen Sie zur Vorderseite des Racks. Installieren Sie auf der linken Seite in der Bohrung an der vorderen Kante des Racks im Steckplatz bei 1 HE, der für die HMC festgelegt ist, eine Klemmmutter.

   Anmerkung: Der Schienensatz umfasst Klemmmuttern sowohl für quadratische als auch für runde Rackbohrungen. Stellen Sie sicher, dass Sie geeignete Klemmmuttern verwenden, die in die Bohrungen des Racks passen.
5. Gehen Sie an die Rückseite des Racks. Installieren Sie auf der linken Seite in der mittleren Bohrung an der vorderen Kante des Racks im Steckplatz bei 1 HE, der für die HMC festgelegt ist, eine Klemmmutter.
6. Führen Sie an der Vorderseite des Racks die folgenden Schritte aus, um die HMC-Trägerschienen im Rack zu installieren:

   a. Richten Sie die Stifte der Trägerschienen über und unter der Klemmmutter aus, die Sie im vorherigen Schritt installiert haben.

   b. Befestigen Sie auf der rechten Seite des Racks den Flansch am Ende der Trägerschiene an der vorderen Kante des Racks, indem Sie in den oberen und unteren Schraubenlöchern M5-Schrauben anbringen. In das mittlere Schraubenloch wird keine Schiene eingesetzt. Stellen Sie sicher, dass bei der Schienenbaugruppe an der Vorderseite des Racks etwas Spielraum gelassen wird, damit die HMC noch eingesetzt werden kann.
7. Ziehen Sie rechts an der Rückseite des Racks das freie Ende der Trägerschiene zur Rückseite und befestigen Sie den Flansch der Trägerschiene am Rack, indem Sie zwei M5-Schrauben anbringen. In das mittlere Schraubenloch wird keine Schraube eingesetzt.
8. Wiederholen Sie die Schritte „6” auf Seite 10 und „7” auf Seite 10, um die Schienenbaugruppe für die linke Trägerschiene an der linken Seite des Racks zu installieren.
9. Führen Sie an der Vorderseite des Racks die folgenden Schritte aus, um die HMC-Workstation im Rack zu installieren:

   a. Halten Sie den Hebel der HMC-Workstation und setzen Sie die inneren Schienen in die HMC-Trägerschienen ein, die Sie im vorherigen Schritt installiert haben. Schieben Sie die HMC nach vorne, bis die Flansche an der Vorderseite der HMC bündig mit den offenen Schraubenlöchern anliegen, die sich an der Vorderseite des Racks befinden.

   b. Befestigen Sie die HMC an der linken Seite des Rahmens mit einer M5-Schraube. Wiederholen Sie diesen Schritt auf der rechten Seite des Racks.

   Anmerkung: Sofern vorhanden, entfernen Sie die orangefarbenen Transporthalterungen, die an der Rückseite des Systems angebracht sind, und bringen Sie die Schraube wieder an.
10. Fahren Sie mit „System im Rack installieren und Netzkabel anschließen und verlegen” auf Seite 10 fort.

System im Rack installieren und Netzkabel anschließen und verlegen

Installieren des Systems auf den Schienen und Anschließen und Verlegen der Netzkabel.

Informationen zu diesem Vorgang

Vorsicht: Dieses Teil oder diese Einheit ist schwer, wiegt jedoch weniger als 18 kg. Beim Anheben, Ausbauen oder Installieren dieses Teils oder dieser Einheit vorsichtig vorgehen. (C008)

Vorgehensweise

1. Entfernen Sie die Schutzfolie aus Plastik von der Oberseite des Systemchassis.
2. Schließen Sie die Netzkabel an die Netzteile an.

   Anmerkung: Schließen Sie das andere Ende des Netzkabels jetzt nicht an den Versorgungsstromkreis an.

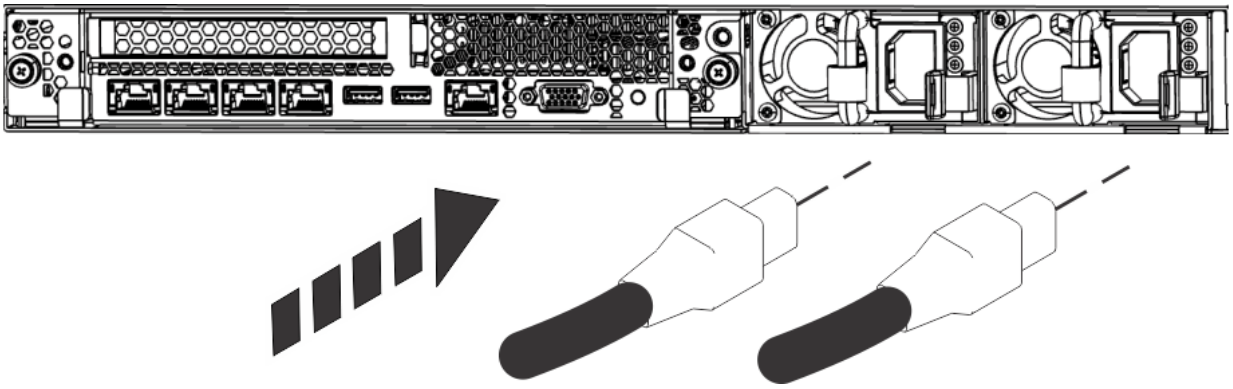


Abbildung 2. Netzkabel an die Netzteile anschließen

3. Befestigen Sie die Klettverschlüsse, um die Netzkabel zu fixieren.
4. Fahren Sie mit „In einem Rack installierte HMC 7063-CR2 verkabeln” auf Seite 11 fort.

In einem Rack installierte HMC 7063-CR2 verkabeln

Hier erfahren Sie, wie Sie Ihre in einem Rack installierte Hardware Management Console (HMC) installieren.

Vorgehensweise

1. Stellen Sie sicher, dass die HMC in einem Rack installiert wurde und die Netzkabel an die Netzteile angeschlossen sind. Weitere Informationen finden Sie unter „System im Rack installieren und Netzkabel anschließen und verlegen” auf Seite 10. Fahren Sie nach der Installation der HMC in einem Rack mit dem nächsten Schritt fort.
2. Schließen Sie Tastatur, Bildschirm und Maus an.

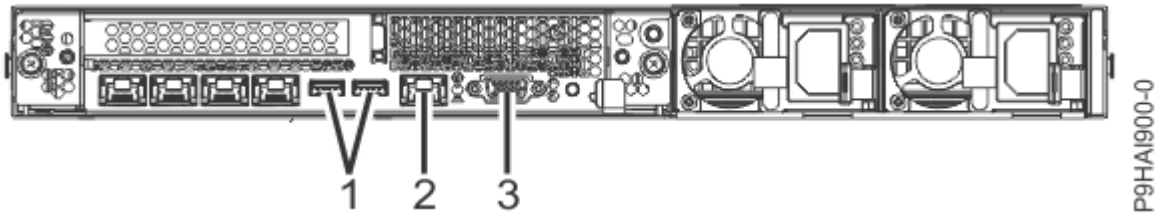


Abbildung 3. Ports an der Rückseite

Tabelle 4. Eingabe- und Ausgabeports

Kennung	**Beschreibung**
1	USB 2.0 für Tastatur und Maus
2	Ethernet Intelligent Platform Management Interface (IPMI)
3	Video Graphics Array (VGA) für den Monitor. Es wird nur die VGA-Einstellung 1024 x 768 bei 60 Hz unterstützt. Zudem werden nur Kabel mit einer Länge bis zu drei Metern unterstützt.

Anmerkung: Das System verfügt über zwei USB-Anschlüsse an der Vorderseite, die Sie verwenden können.

3. Verbinden Sie den Ethernet Intelligent Platform Management Interface(IPMI)-Anschluss mit einem Netz.

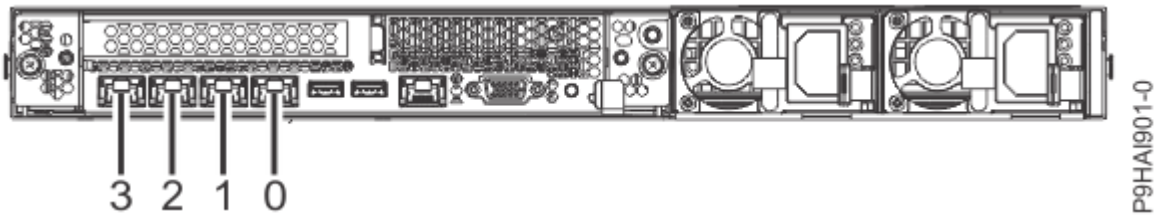


Abbildung 4. Ethernet-Anschlüsse

Tabelle 5. Ethernet-Anschlüsse	
Kennung	**Beschreibung**
0	Gemeinsam genutzte Ethernet Intelligent Platform Management Interface-(IPMI-) und HMC-Netzverbindung
1, 2 und 3	HMC-Netzverbindung

Anmerkung: Diese Verbindung ist für den Zugriff auf den Baseboard-Management-Controller (BMC) auf der HMC erforderlich. Der Zugriff auf den BMC ist für Service-Tasks und für die Verwaltung der HMC-Firmware erforderlich. Weitere Informationen finden Sie unter „Arten von HMC-Netzverbindungen” auf Seite 40.

Warnung: Möglicherweise ist dieses Produkt in Ihrem Land nicht für den Anschluss an Schnittstellen von öffentlichen Telekommunikationsnetzen zertifiziert. Vor der Herstellung einer solchen Verbindung ist eine entsprechende Zertifizierung ggf. gesetzlich vorgeschrieben. Für weitere Informationen wenden Sie sich bitte an IBM.

4. Schließen Sie das Ethernet-Kabel an, das für die Verbindung zum verwalteten System oder zu den verwalteten Systemen bestimmt ist.

   Notes:

   - Wenn Sie für IPMI und HMC eine gemeinsam genutzte Verbindung verwenden, kann ein einzelnes Kabel an Port 0 in Abbildung 2 beide Anforderungen für IPMI und HMC erfüllen.
   - Weitere Informationen über die HMC-Netzverbindungen erhalten Sie unter „HMC-Netzverbindungen” auf Seite 39.
5. Wenn das verwaltete System bereits installiert ist, können Sie prüfen, ob die Ethernet-Kabelverbindung aktiv ist, indem Sie die grünen Statusanzeigen an der HMC und den Ethernet-Anschlüssen des verwalteten Systems während der Installation beobachten.
6. Schließen Sie die Netzkabel des Systems und die Netzkabel für alle anderen angeschlossenen Geräte an die Wechselstromquelle (Alternating Current, AC) an.
7. Prüfen Sie anhand der Netzteil-LEDs den Stromversorgungsstatus. Weitere Informationen hierzu finden Sie unter LEDs im System vom Typ 7063-CR2LEDs im System vom Typ 7063-CR2.
8. Drücken Sie den Netzschalter, um das System zu starten. Die Betriebsanzeige blinkt nicht mehr und leuchtet permanent, was bedeutet, dass das System eingeschaltet ist.

Ergebnisse

Als Nächstes müssen Sie Ihre HMC-Software installieren und konfigurieren. Fahren Sie mit „HMC 7063-CR2 konfigurieren” auf Seite 12 fort.

HMC 7063-CR2 konfigurieren

Hier erfahren Sie, wie Sie die Hardware Management Console (HMC) installieren und konfigurieren.

Überprüfen Sie die HMC-Version, die im Lieferumfang Ihrer HMC enthalten ist. Informationen zum Anzeigen der Version und des Release des HMC-Maschinencodes finden Sie unter HMC-Version überprüfen, die im Lieferumfang Ihrer HMC enthalten ist. Sie können die neueste HMC-Version von der Website Fix Cent-

ral herunterladen. Verwenden Sie austauschbare Datenträger (z. B. DVD oder USB) zum Erstellen einer bootfähigen ISO-Datei mit dem HMC-Paket (ISO-Image).

Anmerkung: In der folgenden Tabelle werden die (vordefinierten) Standard-Anmeldeinformationen für die HMC- und BMC-Schnittstellen beschrieben.

Tabelle 6.

Konsole oder Schnittstelle	Standard-ID	Standardkennwort	Beschreibung
BMC (OpenBMC)	`root`	`0penBmc`	Die Rootbenutzer-ID und das zugehörige Kennwort werden für die erstmalige Anmeldung beim BMC verwendet.
HMC	`hscroot`	`abc123`	Die Benutzer-ID hscroot und das zugehörige Kennwort werden für die erstmalige Anmeldung bei der HMC verwendet. Sie können nur von einem Mitglied der Superadministratorrolle verwendet werden, wobei die Groß-/Kleinschreibung beachtet werden muss.
HMC	`root`	`passw0rd`	Die Benutzer-ID root und das zugehörige Kennwort werden durch den Service-Provider zum Durchführen von Verwaltungsprozeduren verwendet. Sie können nicht für die Anmeldung bei der HMC verwendet werden.

Anmerkung: Folgende Installationen werden als Beispiele dargestellt.

HMC mit einem USB-Flashlaufwerk installieren

Führen Sie bei Linux®-Systemen die folgenden Schritte aus, um die HMC mit einem USB-Flashlaufwerk zu installieren:

Anmerkung: Beispiele für verschiedene Betriebssysteme finden Sie unter:

- Windows: USB-Flashlaufwerk als Installationsmedium (Windows)
- Mac: USB-Flashlaufwerk als Installationsmedium (macOS)

1. Laden Sie die gewünschte HMC-Version von der Website Fix Central herunter.
2. Führen Sie folgenden Befehl aus: **`dd bs=4M if=/path/to/HMC_ISO_FILE.iso of=/dev/sdx status=progress && sync`** (dabei steht **`sdx`** für den Namen des USB-Laufwerks).

   Anmerkung: Sie können den Linux-Befehl `lsblk` ausführen, um den Gerätenamen des USB-Laufwerks zu ermitteln, wenn dieses angeschlossen ist.
3. Legen Sie das USB-Laufwerk ein und schalten Sie das System ein.

Anmerkung: Das USB-Laufwerk muss einen Speicherplatz von mindestens 8 GB aufweisen. Bestimmte USB-Laufwerke sind möglicherweise zu breit, um ordnungsgemäß in den USB-Anschluss an der Rückseite des Systems zu passen. Testen Sie die Eignung Ihres USB-Laufwerks, bevor Sie fortfahren.

4. Wenn das Menü "Petitboot" angezeigt wird, dann wählen Sie die Option **Hardware Management Console installieren** aus, die sich unter **USB** befindet.

HMC mit einem virtuellen Datenträger über den BMC installieren

Führen Sie die folgenden Schritte aus, um die HMC mit einem virtuellen Datenträger über den BMC zu installieren:

1. Öffnen Sie einen unterstützten Web-Browser. Geben Sie in der Adressleiste die IP-Adresse des BMC ein, zu dem Sie eine Verbindung herstellen möchten. Sie können in der Adressleiste des Web-Browsers beispielsweise das Format `https://<BMC-IP>` verwenden.
2. Geben Sie im Fenster "**OpenBMC-Anmeldung**" die **Hostadresse** des BMC und den **Benutzernamen** und das **Kennwort** ein, die Ihnen zugewiesen sind.

   Anmerkung: Die Standard-Benutzer-ID lautet `root` und das Standardkennwort `0penBmc`.

   Wenn Sie Firmware ab Version OP940.01 verwenden, ist das Rootkennwort standardmäßig abgelaufen. Sie müssen das Standardkennwort ändern, bevor Sie auf den BMC zugreifen können. Weitere Informationen zum Ändern des abgelaufenen Standardkennworts finden Sie unter Kennwort festlegen.

   Wenn Sie Ihr Kennwort vergessen haben, können Sie das System auf die Werkseinstellungen zurücksetzen, um das Standardkennwort wiederherzustellen. Informationen zum Zurücksetzen des Systems finden Sie unter Zurücksetzung auf Werkseinstellungen durchführen.
3. Klicken Sie auf **Anmelden**.
4. Wählen Sie **Serversteuerung** aus.
5. Wählen Sie **Virtueller Datenträger** aus.
6. Klicken Sie auf **Datei auswählen**.
7. Suchen Sie den ISO-Wiederherstellungsdatenträger der HMC und klicken Sie auf **Öffnen**.
8. Klicken Sie auf **Starten**.
9. Schalten Sie das System ein.
10. Wenn das Menü "Petitboot" angezeigt wird, dann wählen Sie die Option **Hardware Management Console installieren** aus, die sich unter **USB** befindet.

HMC mit einem über USB angeschlossenen externen DVD-Laufwerk installieren

Führen Sie die folgenden Schritte aus, um die HMC mit einem über USB angeschlossenen externen DVD-Laufwerk zu installieren:

1. Laden Sie die gewünschte HMC-Wiederherstellungsversion von der Website Fix Central herunter.
2. Brennen Sie das DVD-Image für die Wiederherstellung der HMC als Image auf einen DVD-R-DL-Datenträger.
3. Schalten Sie die HMC aus.
4. Schließen Sie das externe USB-DVD-Laufwerk an die HMC an und legen Sie die HMC-Wiederherstellungs-DVD ein.

   Anmerkung: Möglicherweise müssen Sie das USB-DVD-Laufwerk an eine externe Stromquelle anschließen oder ein USB-Y-Kabel verwenden, um eine Verbindung zu einem zusätzlichen USB-Anschluss herzustellen, der ausreichend Strom für das DVD-Laufwerk liefert.
5. Schalten Sie die HMC ein.

   Anmerkung: Auf dem Anzeigemonitor wird beim Start möglicherweise kein Signal angezeigt. Es kann 2 oder 3 Minuten dauern, bis auf dem Anzeigemonitor ein Status angezeigt wird.

6. Wenn das Bootladeprogramm Petitboot gestartet wird, navigieren Sie zum Stoppen des automatischen Bootens.

   Anmerkung: Es wird ein Zeitlimit von 10 Sekunden erzwungen. Wenn innerhalb dieser 10 Sekunden keine Aktion erfolgt, versucht das System, vom Festplattenlaufwerk zu booten.

7. Warten Sie, bis die **CD/DVD**-Einheit im Menü "Petitboot" angezeigt wird.

   Anmerkung: Dieser Prozess kann bis zu einer Minute dauern.

8. Wählen Sie die Option **Hardware Management Console installieren** aus, die sich unter **CD/DVD** befindet.

7063-CR1 in einem Rack installieren

Hier erfahren Sie, wie Sie die Hardware Management Console (HWM) 7063-CR1 in einem Rack installieren.

Sie können die Installationsdokumentation online anzeigen oder die PDF-Version mit denselben Informationen drucken. Informationen zum Anzeigen oder Drucken der PDF-Version finden Sie unter Hardware Management Console installieren und konfigurieren.

Voraussetzungen für die Installation des Einschubsystems vom Typ 7063-CR1

Hier finden Sie Informationen zu den Voraussetzungen, die für die Installation des Systems erforderlich sind.

Informationen zu diesem Vorgang

Vorsicht:

oder

oder

Dieses Teil oder diese Einheit wiegt zwischen 18 und 32 kg. Zum Anheben dieses Teils oder dieser Einheit sind zwei Personen erforderlich. (C009)

Bevor Sie mit der Installation des Servers beginnen, sollten Sie die folgenden Dokumente lesen:

- Die aktuelle Version dieses Dokuments wird online verwaltet. Siehe 7063-CR1 in einem Rack installieren (http://www.ibm.com/support/knowledgecenter/POWER9/p9hai/p9hai_install7063_kickoff.htm).
- Informationen zur Planung Ihrer Serverinstallation finden Sie unter Standort- und Hardwareplanung.

Vorgehensweise

Vergewissern Sie sich, dass Sie vor Beginn der Installation Folgendes zur Hand haben:

- Kreuzschlitz-Schraubendreher der Größe 2
- Schlitzschraubendreher
- Teppichmesser
- Antistatikarmband zum Schutz vor elektrostatischer Entladung
- Rack mit einer freien EIA-Einheit (1U)

Anmerkung: Ist kein Rack installiert, installieren Sie das Rack. Entsprechende Anweisungen finden Sie unter Racks und Rack-Features (http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_9xx_kickoff.htm).

Bestandsaufnahme für Ihr System ausführen

Verwenden Sie diese Informationen, um eine Bestandsaufnahme für Ihr System auszuführen.

Vorgehensweise

1. Überprüfen Sie, ob Sie alle bestellten Pakete erhalten haben.
2. Packen Sie die Serverkomponenten aus.
3. Führen Sie vor der Installation jeder Serverkomponente eine Bestandsaufnahme durch und überprüfen Sie, ob Sie alle bestellten Teile erhalten haben.

   Anmerkung:

   Die Bestellinformationen sind Teil des Produkts. Bestellinformationen können Sie auch über den Vertriebsbeauftragten oder den IBM Business Partner erhalten.

   Ist die Lieferung falsch, fehlen Teile oder sind Teile beschädigt, wenden Sie sich an eine der folgenden Stellen:

   - IBM Reseller.
   - In den USA unter der Telefonnummer 1-800-300-8751 an die IBM Rochester Manufacturing Automated Information Line.
   - Website mit dem Verzeichnis der weltweiten Kontakte (http://www.ibm.com/planetwide). Wählen Sie Ihren Standort aus, um die Kontaktinformationen für Service und Support aufzurufen.

Position im Rack für das System vom Typ 7063-CR1 bestimmen und markieren

Möglicherweise müssen Sie die Position bestimmen, an der die Systemeinheit im Rack installiert werden soll.

Vorgehensweise

1. Lesen Sie die Racksicherheitshinweise (http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_racksafety.htm).
2. Ermitteln Sie, wo die Systemeinheit im Rack angeordnet werden soll. Berücksichtigen Sie bei der Planung der Installation der Systemeinheit in einem Rack die folgenden Informationen:
   - Ordnen Sie große und schwere Einheiten im unteren Bereich des Racks an.
   - Planen Sie, Systemeinheiten zunächst im unteren Bereich des Racks zu installieren.
   - Erfassen Sie die EIA-Positionen (EIA = Electronic Industries Alliance) in Ihrem Plan.
3. Falls erforderlich, bauen Sie die Abdeckblenden aus, um auf die Positionen im Inneren des Rackschranks zugreifen zu können, an denen die Einheiten installiert werden sollen, wie in Abbildung 5 auf Seite 17 dargestellt.

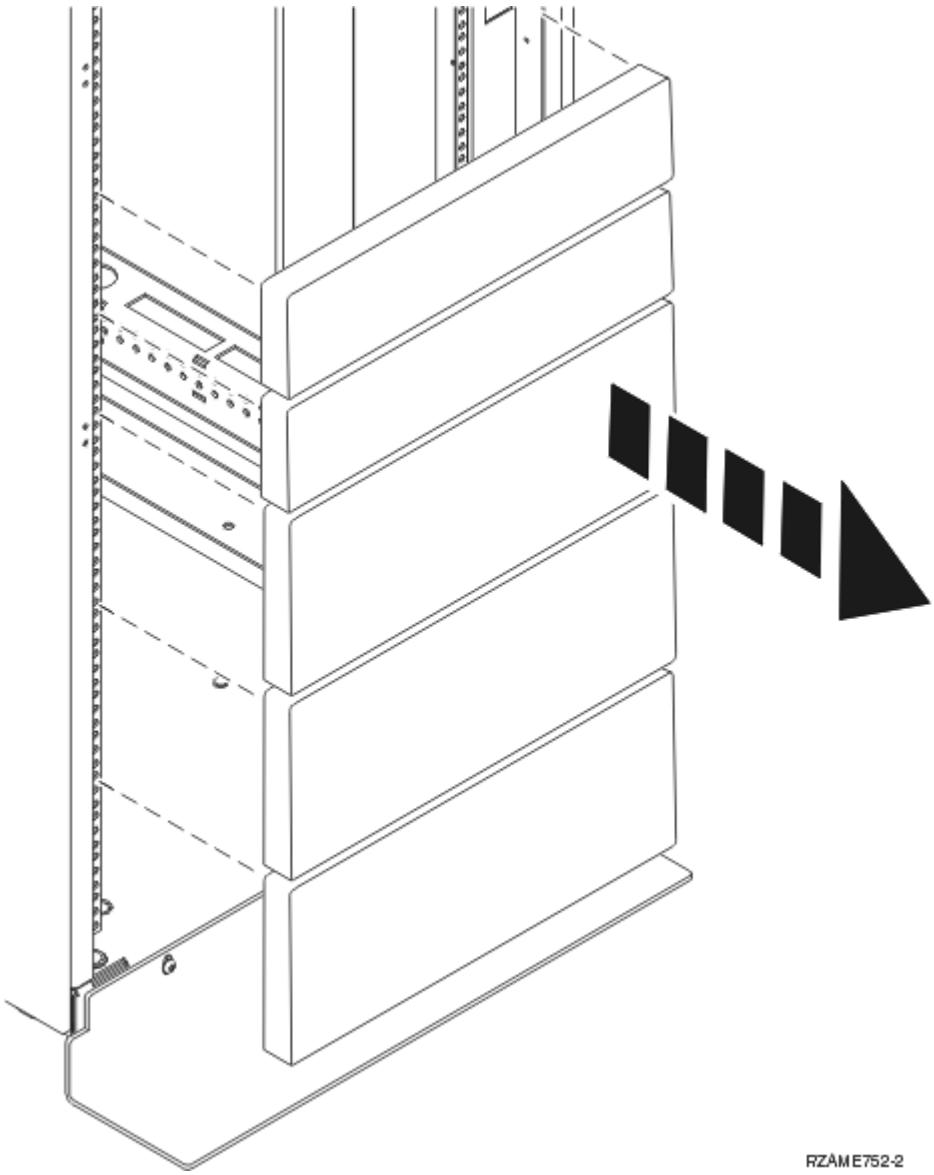


Abbildung 5. Abdeckblenden ausbauen

4. Bestimmen Sie die Position des Systems im Rack. Notieren Sie die EIA-Position.
5. Stellen Sie sich vor die Vorderseite des Racks und markieren Sie auf der rechten Seite mithilfe eines Bandes, eines Markers oder eines Stiftes die niedrigere Bohrung der einzelnen EIA-Einheiten.
6. Wiederholen Sie Schritt „5” auf Seite 17 für die entsprechenden Löcher auf der linken Seite des Racks.
7. Gehen Sie an die Rückseite des Racks.
8. Suchen Sie auf der rechten Seite die EIA-Einheit, die der auf der Vorderseite des Racks gekennzeichneten unteren EIA-Einheit entspricht.
9. Markieren Sie die untere EIA-Einheit.
10. Markieren Sie die entsprechenden Löcher auf der linken Seite des Racks.

Fixierte Schienen am Systemchassis und am Rack anbringen

Sie müssen die Schienen auf dem Chassis und am Rack installieren. Verwenden Sie für diese Aufgabe das folgende Verfahren.

Informationen zu diesem Vorgang

Achtung: Um Fehler an der Schienenführung und mögliche Gefahren für Sie und die Einheit zu vermeiden, muss darauf geachtet werden, dass die korrekten Schienen und Verbindungsstücke für das Rack benutzt werden. Die Schienen im Rack haben quadratische oder runde Flanschbohrungen. Achten Sie darauf, dass die Schienen und Verbindungsstücke den Flanschbohrungen im Rack entsprechen. Bei nicht passenden Teilen keine Unterlegscheiben oder Abstandshalter verwenden. Sind die korrekten Schienen und Verbindungsstücke für das Rack nicht vorhanden, wenden Sie sich an Ihren IBM Reseller.

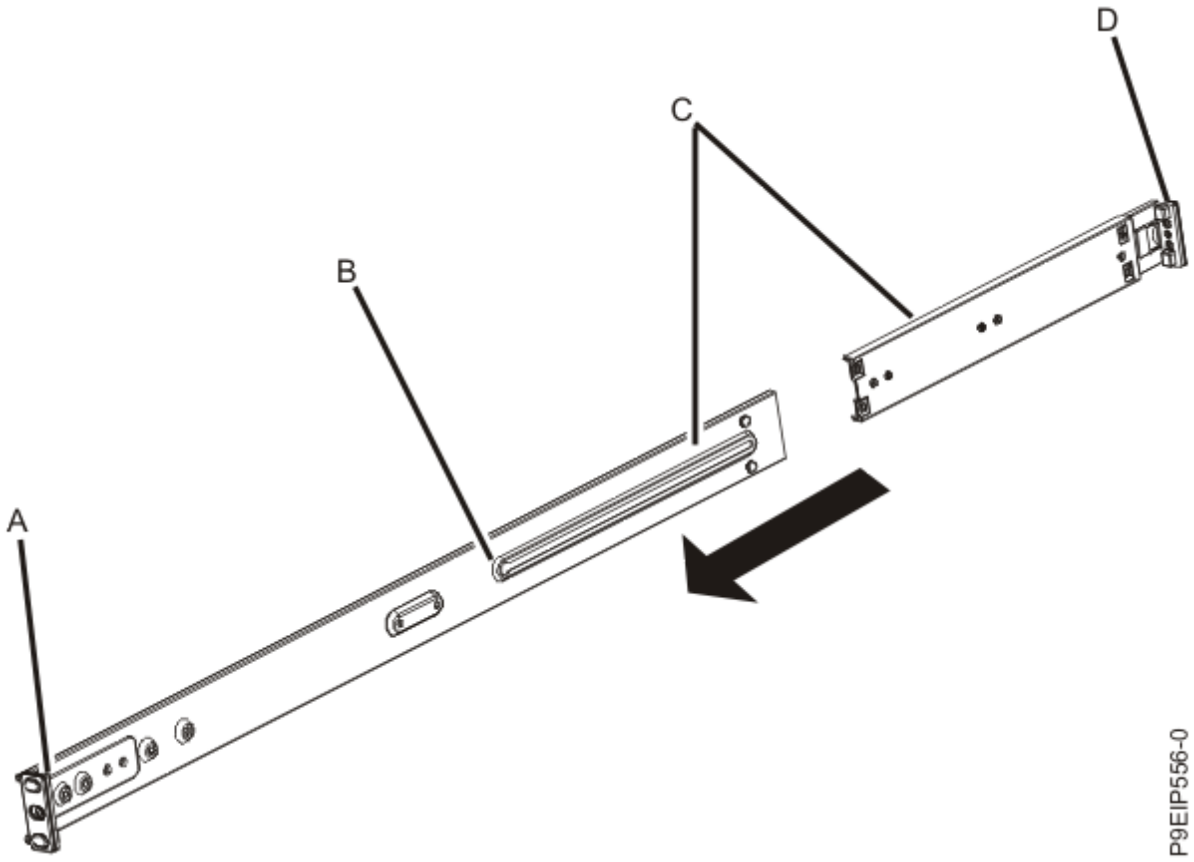
Anmerkung: Für das System ist 1 EIA-Rackeinheit (1U) an Platz erforderlich.

Stellen Sie sicher, dass Sie über alle Teile verfügen, die Sie für die Installation der Schienen benötigen. Folgende Teile sind im Schienensatz enthalten:

- Schrauben der Schienen zum Anbringen der aus zwei Teilen bestehenden Schienen
- Schrauben des Racks für die Schienen zum Befestigen der Schienen am Rack
- Schienen
- Schrauben vom Typ 10 - 32 x 0,635 cm (0,25 Zoll) zum Anbringen der Schienen am Systemchassis

Vorgehensweise

1. Nehmen Sie die Teile der Schienen aus der Verpackung und legen Sie sie auf eine Arbeitsoberfläche.
2. Tauschen Sie die Viereckstifte (**A**) und (**D**) gegen die Rundstifte aus.
3. Verbinden Sie die zwei Teile der Rackschienen miteinander. Führen Sie die folgenden Schritte aus, um die zwei Teile der Rackschienen miteinander zu verbinden:
   a. Bestimmen Sie die zwei Teile der linken Rackschiene. Richten Sie die kurzen und langen Teile aus (**C**). Stellen Sie sicher, dass die Stifte an den Rackschienen in die gleiche Richtung zeigen (**A** und **D**).



b. An dem kürzeren Teil der Rackschiene befindet sich ein Metallstift. Setzen Sie den Stift in die Bohrung an dem längeren Teil der Rackschiene ein (**B**). Schieben Sie das kürzere Teil der Rackschiene in das längere Teil der Rackschiene.

c. Richten Sie die Bohrungen in den zwei Teilen der Rackschiene aus. Bringen Sie die zwei Teile mit einem Kreuzschlitz-Schraubendreher an, indem Sie zwei mit Gewinde versehenen Schrauben der Schiene in den Bohrungen an der Rackschiene leicht anziehen.

Anmerkung: Ziehen Sie die Schrauben der Rackschienen nicht fest.

d. Wiederholen Sie diese Schritte für die rechte Schiene.

4. Installieren Sie die Rackschienen am Rack.

a. Gehen Sie zur Vorderseite des Racks.

b. Wählen Sie die linke Rackschiene aus und suchen Sie die EIA-Einheit, die Sie zuvor markiert haben. Zur Bestimmung der Rückseite des Racks sind die einzelnen Schienen zudem mit **Rückseite** markiert. Stellen Sie sicher, dass Sie die Vorderseite der Rackschiene in der Hand halten.

c. Ziehen Sie die Schiene von der Vorderseite des Racks bis zur Rückseite des Racks aus und richten Sie die Stifte der Rackschiene an den Bohrungen im Rackflansch aus, den Sie zuvor markiert haben.

d. Drücken Sie die Stifte der Rackschiene so weit in die Rückseite des Rackflansches, bis die hintere Verriegelung der Rackschiene einrastet.

e. Ziehen Sie die Vorderseite der Rackschiene in Richtung der Vorderseite des Rackflansches. Richten Sie die Schienenstifte an den Bohrungen im Rackflansch aus und ziehen Sie daran, bis die Verriegelung der Schiene einrastet.

f. Ziehen Sie die Schrauben, die Sie in Schritt 2 eingesetzt haben, mit einem Schraubendreher fest.

Anmerkung: Möglicherweise benötigen Sie 2 Einheiten (2U) Platz, um an die Schrauben der Schiene zu gelangen und sie festzuziehen.

g. Wiederholen Sie die Schritte 4a bis 4f für die rechte Schiene.

System im Rack installieren und Netzkabel anschließen und verlegen

Installieren des Systems auf den Schienen und Anschließen und Verlegen der Netzkabel.

Informationen zu diesem Vorgang

Vorsicht:

oder

oder

Dieses Teil oder diese Einheit wiegt zwischen 18 und 32 kg. Zum Anheben dieses Teils oder dieser Einheit sind zwei Personen erforderlich. (C009)

Vorgehensweise

1. Entfernen Sie die Schutzfolie aus Plastik von der Oberseite des Systemchassis.
2. Gehen Sie zur Vorderseite des Racks.
3. Heben Sie das System mit zwei Personen an und richten Sie die Schienen des Systemchassis an den Seiten des Chassis an den Schienen des Racks aus.
4. Schieben Sie das System vorsichtig in Richtung der Rückseite des Racks.

5. Befestigen Sie das System am Rack, indem Sie an den Seiten des Systemchassis jeweils eine Schraube mit Unterlegscheibe an den Griffen anbringen.

   Anmerkung: Bei den Schrauben müssen Sie Unterlegscheiben verwenden. Schieben Sie eine Unterlegscheibe auf jede der beiden längeren Schrauben (1,5 cm), die im Schienensatz enthalten sind. Drehen Sie die Schraube mit der Unterlegscheibe durch die rechte und linke Seite an der Vorderseite des Systems ein.
6. Schließen Sie die Netzkabel an die Netzteile an.

   Anmerkung: Schließen Sie das andere Ende des Netzkabels jetzt nicht an den Versorgungsstromkreis an.

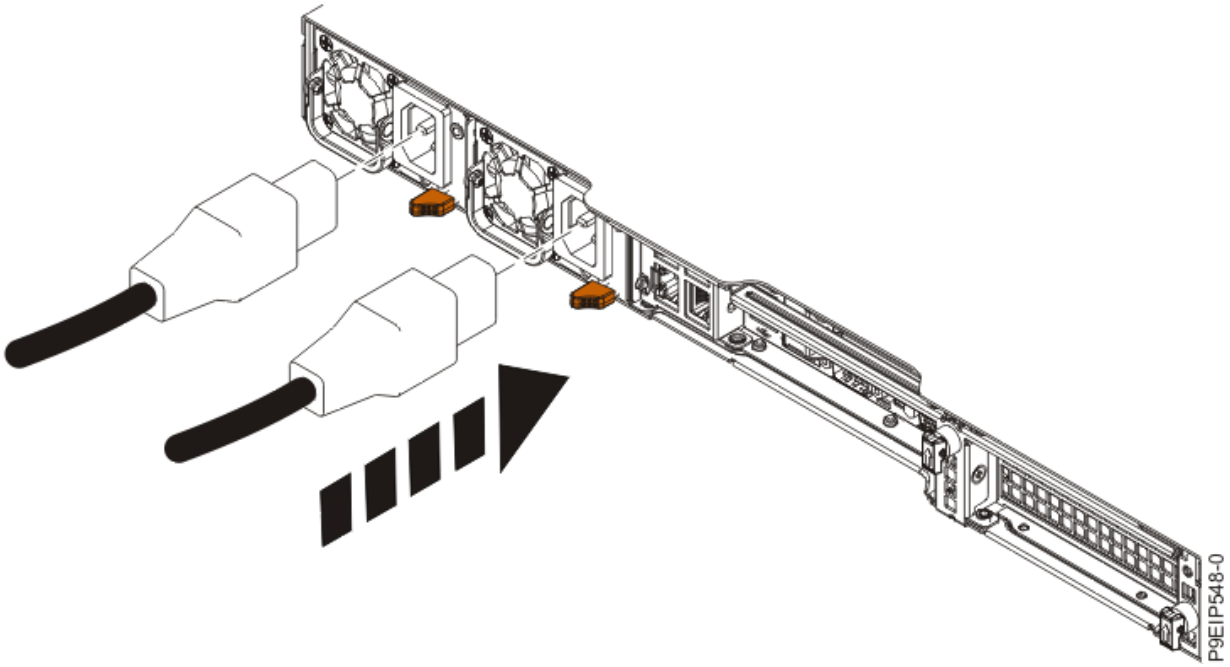


Abbildung 6. Netzkabel an die Netzteile anschließen

7. Fahren Sie mit „In einem Rack installierte HMC 7063-CR1 verkabeln” auf Seite 20 fort.

In einem Rack installierte HMC 7063-CR1 verkabeln

Hier erfahren Sie, wie Sie Ihre in einem Rack installierte Hardware Management Console (HMC) installieren.

Vorgehensweise

1. Stellen Sie sicher, dass die HMC in einem Rack installiert wurde und die Netzkabel an die Netzteile angeschlossen sind. Weitere Informationen finden Sie unter „System im Rack installieren und Netzkabel anschließen und verlegen” auf Seite 19. Fahren Sie nach der Installation der HMC in einem Rack mit dem nächsten Schritt fort.

   Anmerkung: Falls ein Stecker an der Rückseite des Systems einen Anschluss abdeckt, den Sie verwenden müssen, entfernen Sie diesen und legen Sie ihn zur Seite. Durch die Anschlussabdeckungen wird sichergestellt, dass Sie daran denken, beim einleitenden Programmladen des Systems das Administratorkennwort für Ihr verwaltetes System zurückzusetzen.
2. Schließen Sie Tastatur, Bildschirm und Maus an.

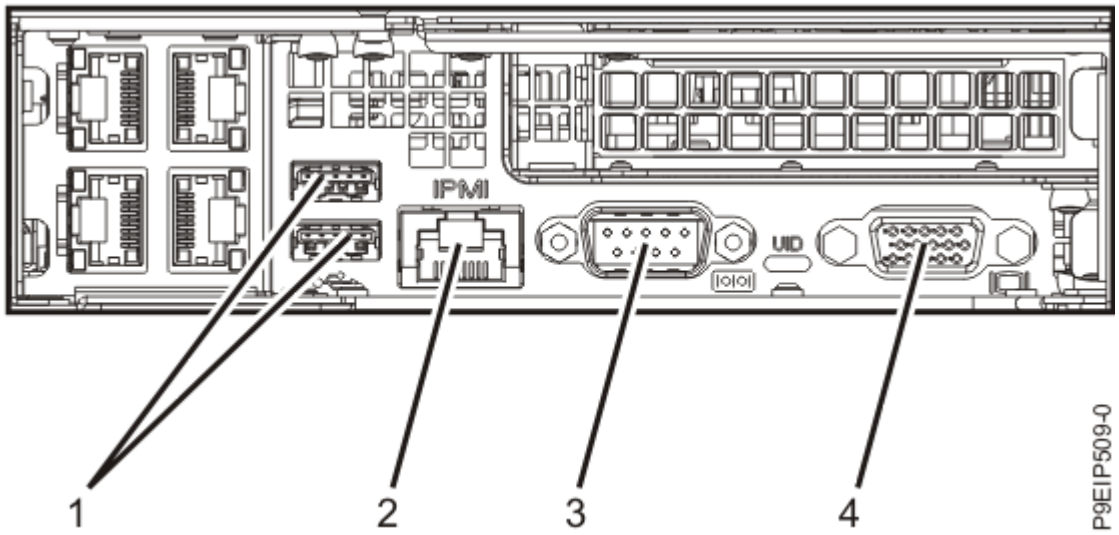


Abbildung 7. Ports an der Rückseite

Tabelle 7. Eingabe- und Ausgabeports	
Kennung	**Beschreibung**
1	USB 2.0 für Tastatur und Maus
2	Ethernet Intelligent Platform Management Interface (IPMI)
3	Serielle IPMI
4	Video Graphics Array (VGA) für den Monitor. Es wird nur die VGA-Einstellung 1024 x 768 bei 60 Hz unterstützt. Zudem werden nur Kabel mit einer Länge bis zu drei Metern unterstützt.

Anmerkung: Das System verfügt über zwei USB-Anschlüsse an der Vorderseite, die Sie verwenden können. Der vordere serielle Anschluss ist nicht funktionsfähig.

3. Schließen Sie das Ethernet-Kabel an, das für die Verbindung zum verwalteten System oder zu den verwalteten Systemen bestimmt ist.

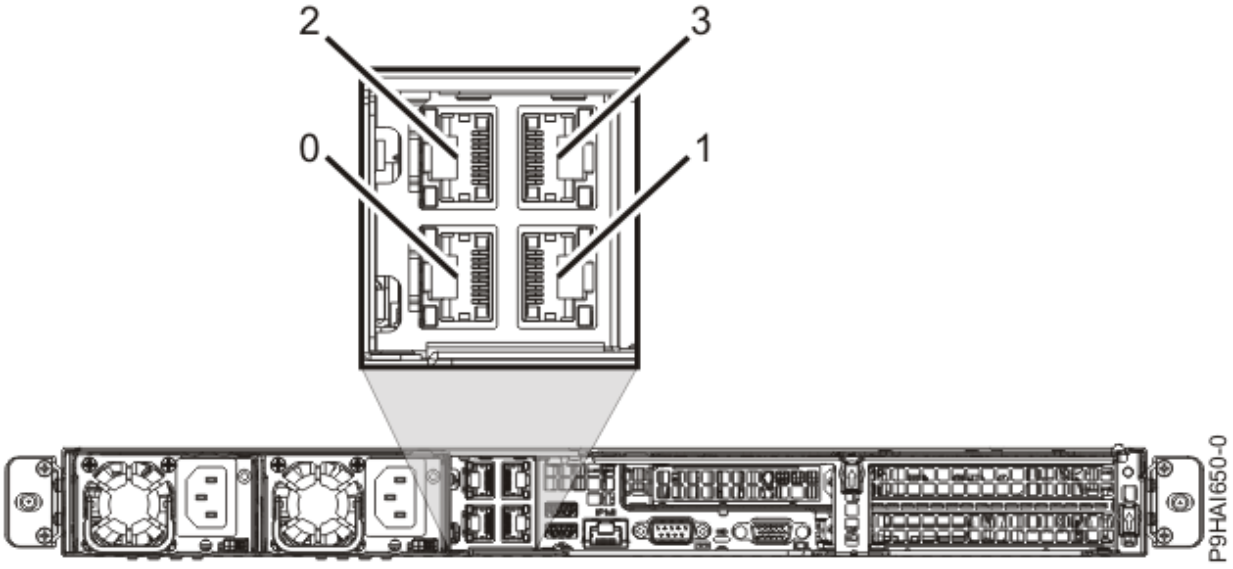


Abbildung 8. Ethernet-Anschlüsse

Anmerkung: Weitere Informationen über die HMC-Netzverbindungen erhalten Sie unter „HMC-Netzverbindungen” auf Seite 39.

4. Wenn das verwaltete System bereits installiert ist, können Sie prüfen, ob die Ethernet-Kabelverbindung aktiv ist, indem Sie die grünen Statusanzeigen an der HMC und den Ethernet-Anschlüssen des verwalteten Systems während der Installation beobachten.
5. Verbinden Sie den Ethernet Intelligent Platform Management Interface(IPMI)-Anschluss mit einem Netz.

   Anmerkung: Diese Verbindung ist für den Zugriff auf den Baseboard-Management-Controller (BMC) auf der HMC erforderlich. Der Zugriff auf den BMC ist für Service-Tasks und für die Verwaltung der HMC-Firmware erforderlich. Weitere Informationen finden Sie unter „Arten von HMC-Netzverbindungen” auf Seite 40.

6. Schließen Sie die Netzkabel des Systems und die Netzkabel für alle anderen angeschlossenen Geräte an die Wechselstromquelle (Alternating Current, AC) an.
7. Prüfen Sie anhand der Netzteil-LEDs den Stromversorgungsstatus. Weitere Informationen hierzu finden Sie unter LEDs im System vom Typ 7063-CR1LEDs im System vom Typ 7063-CR1.

Ergebnisse

Als Nächstes müssen Sie Ihre HMC-Software installieren und konfigurieren. Fahren Sie mit „HMC 7063-CR1 konfigurieren” auf Seite 22 fort.

HMC 7063-CR1 konfigurieren

Hier erfahren Sie, wie Sie die Hardware Management Console (HMC) installieren und konfigurieren.

Überprüfen Sie die HMC-Version, die im Lieferumfang Ihrer HMC enthalten ist. Sie können die neueste HMC-Version von der Website Fix Central herunterladen. Verwenden Sie austauschbare Datenträger (z. B. DVD oder USB) zum Erstellen einer bootfähigen ISO-Datei mit dem HMC-Paket (ISO-Image).

Anmerkung: In der folgenden Tabelle werden die (vordefinierten) Standard-Anmeldeinformationen für die HMC- und BMC-Schnittstellen beschrieben.

Tabelle 8.

Konsole oder Schnittstelle	Standard-ID	Standardkennwort	Beschreibung
BMC	`ADMIN`	`ADMIN`	Die Benutzer-ID ADMIN und das zugehörige Kennwort werden für die erstmalige Anmeldung beim BMC verwendet.
HMC	`hscroot`	`abc123`	Die Benutzer-ID hscroot und das zugehörige Kennwort werden für die erstmalige Anmeldung bei der HMC verwendet. Sie können nur von einem Mitglied der Superadministratorrolle verwendet werden, wobei die Groß-/Kleinschreibung beachtet werden muss.

Tabelle 8. (Forts.)

Konsole oder Schnittstelle	Standard-ID	Standardkennwort	Beschreibung
HMC	`root`	`passw0rd`	Die Benutzer-ID root und das zugehörige Kennwort werden durch den Service-Provider zum Durchführen von Verwaltungsprozeduren verwendet. Sie können nicht für die Anmeldung bei der HMC verwendet werden.

Anmerkung: Folgende Installationen werden als Beispiele dargestellt.

HMC mit einem USB-Flashlaufwerk installieren

Führen Sie bei Linux-Systemen die folgenden Schritte aus, um die HMC mit einem USB-Flashlaufwerk zu installieren:

Anmerkung: Beispiele für verschiedene Betriebssysteme finden Sie unter:

- Windows: USB-Flashlaufwerk als Installationsmedium (Windows)
- Mac: USB-Flashlaufwerk als Installationsmedium (macOS)

1. Laden Sie die gewünschte HMC-Version von der Website Fix Central herunter.
2. Führen Sie folgenden Befehl aus: **`dd bs=4M if=/path/to/HMC_ISO_FILE.iso of=/dev/sdx status=progress && sync`** (dabei steht **`sdx`** für den Namen des USB-Laufwerks).

   Anmerkung: Sie können den Linux-Befehl `lsblk` ausführen, um den Gerätenamen des USB-Laufwerks zu ermitteln, wenn dieses angeschlossen ist.
3. Legen Sie das USB-Laufwerk ein und schalten Sie das System ein.

   Anmerkung: Das USB-Laufwerk muss einen Speicherplatz von mindestens 4 GB aufweisen. Bestimmte USB-Laufwerke sind möglicherweise zu breit, um ordnungsgemäß in den USB-Anschluss an der Rückseite des Systems zu passen. Testen Sie die Eignung Ihres USB-Laufwerks, bevor Sie fortfahren.
4. Wenn das Menü "Petitboot" angezeigt wird, dann wählen Sie die Option **Hardware Management Console installieren** aus, die sich unter **USB** befindet.

HMC mit einem fernen Datenträger über die Anzeigefunktion der Konsole installieren

Führen Sie die folgenden Schritte aus, um die HMC mit einem fernen Datenträger über die Anzeigefunktion der Konsole zu installieren:

1. Melden Sie sich bei der BMC-Webschnittstelle an (`http://<bmc-ip>`).
2. Wählen Sie **Fernsteuerung** aus.
3. Wählen Sie **Konsolenumleitung** aus.
4. Klicken Sie auf **Konsole starten**.
5. Wählen Sie im Java™ iKVM Viewer den Eintrag **Virtueller Datenträger** > **Virtueller Speicher** aus.
6. Wählen Sie unter **Typ des logischen Laufwerks** den Eintrag **ISO-Datei** aus.
7. Klicken Sie auf **Image öffnen** und suchen Sie die ISO-Datei auf Ihrem System.
8. Klicken Sie auf **Plug-in**, um die ISO-Datei anzuhängen.
9. Schalten Sie das System ein.

10. Wenn das Menü "Petitboot" angezeigt wird, dann wählen Sie die Option **Hardware Management Console installieren** aus, die sich unter **CD/DVD** befindet.

HMC mit einem über USB angeschlossenen externen DVD-Laufwerk installieren

Führen Sie die folgenden Schritte aus, um die HMC mit einem über USB angeschlossenen externen DVD-Laufwerk zu installieren:

1. Laden Sie die gewünschte HMC-Wiederherstellungsversion von der Website Fix Central herunter.
2. Brennen Sie das DVD-Image für die Wiederherstellung der HMC als Image auf einen DVD-R-Datenträger. Alternativ können Sie den Wiederherstellungsdatenträger auf DVD bestellen.
3. Schalten Sie die HMC aus.
4. Schließen Sie das externe USB-DVD-Laufwerk an die HMC an und legen Sie die HMC-Wiederherstellungs-DVD ein.

   Anmerkung: Möglicherweise müssen Sie das USB-DVD-Laufwerk an eine externe Stromquelle anschließen oder ein USB-Y-Kabel verwenden, um eine Verbindung zu einem zusätzlichen USB-Anschluss herzustellen, der ausreichend Strom für das DVD-Laufwerk liefert.
5. Schalten Sie die HMC ein.

   Anmerkung: Auf dem Anzeigemonitor wird beim Start möglicherweise kein Signal angezeigt. Es kann 2 oder 3 Minuten dauern, bis auf dem Anzeigemonitor ein Status angezeigt wird.
6. Wenn das Bootladeprogramm Petitboot gestartet wird, navigieren Sie zum Stoppen des automatischen Bootens.

   Anmerkung: Es wird ein Zeitlimit von 10 Sekunden erzwungen. Wenn innerhalb dieser 10 Sekunden keine Aktion erfolgt, versucht das System, vom Festplattenlaufwerk zu booten.
7. Warten Sie, bis die **CD/DVD**-Einheit im Menü "Petitboot" angezeigt wird.

   Anmerkung: Dieser Prozess kann bis zu einer Minute dauern.
8. Wählen Sie die Option **Hardware Management Console installieren** aus, die sich unter **CD/DVD** befindet.

HMC mit einem fernen Datenträger, der von einem SMB-Dateiserver gehostet wird, installieren

Führen Sie die folgenden Schritte aus, um die HMC mit einem fernen Datenträger, der von einem SMB-Dateiserver (Server Message Block) gehostet wird, zu installieren:

1. Kopieren Sie die ISO-Wiederherstellungsdatei auf einen Freigabehost auf Ihrem SMB-kompatiblen Dateiserver.

   Anmerkung: Server Message Block Version 3 (SMBv3) wird nicht unterstützt.
2. Melden Sie sich bei der BMC-Webschnittstelle an (`http://<bmc-ip>`).
3. Wählen Sie **Virtueller Datenträger** aus.
4. Wählen Sie **CD-ROM-Image** aus.
5. Vervollständigen Sie folgende Informationen:

   Freigabehost

   Die IP-Adresse des SMB-Hosts. Stellen Sie bei Verwendung des Hostnamens sicher, dass das Domain Name System (DNS) auf dem BMC ordnungsgemäß konfiguriert wurde.

   Pfad zum Image

   Der SMB-Pfad zum System. Beispiel: `/<Freigabename>/<restlicher Pfad>/<ISO-Name>.iso`

Benutzer (optional)

Der Benutzername, der für die Anmeldung beim SMB-Host verwendet wird.

Kennwort (optional)

Das Kennwort des Benutzers.

6. Klicken Sie auf **Speichern**.
7. Klicken Sie auf **Anhängen**.
8. Einheit 1 zeigt jetzt folgende Nachricht an: **Es wurde eine ISO-Datei angehängt.**

   Anmerkung: Überprüfen Sie die Informationen erneut und wiederholen Sie die Schritte 6 bis 8, wenn die Nachricht nicht angezeigt wird.
9. Schalten Sie das System ein.
10. Wenn das Menü "Petitboot" angezeigt wird, dann wählen Sie die Option **Hardware Management Console installieren** aus, die sich unter **CD/DVD** befindet.

Optional: Aktualisieren Sie die HMC-Firmwareversion mithilfe des im Lieferumfang enthaltenen USB-Memory-Key

Anmerkung: Führen Sie die folgenden Schritte zur Aktualisierung der HMC-Firmwareversion aus, wenn Ihre Konfiguration ein HMC-Firmware-Update auf einem USB-Memory-Key umfasst.

Führen Sie die folgenden Schritte aus, um die HMC-Firmwareversion mithilfe des im Lieferumfang enthaltenen USB-Memory-Key zu aktualisieren:

1. Legen Sie das USB-Memory-Key-Laufwerk in den USB-Anschluss an der Rückseite des Systems ein.
2. Schalten Sie das System ein und melden Sie sich bei der HMC an.
3. Klicken Sie im Navigationsbereich auf das Symbol **HMC-Verwaltung**  und wählen Sie anschließend **Konsolenverwaltung** aus.
4. Klicken Sie im Inhaltsbereich auf **Hardware Management Console aktualisieren**.
5. Befolgen Sie die Anweisungen auf dem Bildschirm im Assistenten "HMC-Fehlerberichtigung installieren".

Als Nächstes müssen Sie Ihre HMC-Software konfigurieren. Anweisungen dazu finden Sie unter „HMC konfigurieren” auf Seite 39.

Zugehörige Konzepte

BMC-Konnektivität konfigurieren

Sie können die Netzeinstellungen auf dem BMC für die Managementkonsole konfigurieren oder anzeigen.

Virtuelle HMC-Appliance installieren

Hier erfahren Sie, wie Sie die Virtuelle Hardware Management Console (HMC)-Appliance installieren.

Die Virtuelle HMC-Appliance kann in Ihrer bestehenden virtualisierten x86- oder POWER-Infrastruktur installiert werden. Die Virtuelle HMC-Appliance unterstützt folgende x86-Virtualisierungshypervisoren:

- Kernelbasierte virtuelle Maschine (KVM)
- Xen
- VMware

Die Virtuelle HMC-Appliance unterstützt folgende POWER-Virtualisierungshypervisoren:

- PowerVM

Mindestvoraussetzungen für die Ausführung der Virtuelle HMC-Appliance:

- 16 GB Hauptspeicher

- 4 virtuelle Prozessoren
- 2 Netzschnittstellen (maximal 4 zulässig)
- 1 Plattenlaufwerk mit 500 GB an verfügbarem Plattenspeicherplatz

Notes:

- Der Prozessor der Systeme, auf denen die Virtuelle HMC-Appliance gehostet wird, muss entweder ein Intel VT-x-Prozessor oder ein AMD-V-Prozessor mit aktivierter Hardwarevirtualisierung sein.
- Die Virtuelle HMC-Appliance-DVDs, die Sie erhalten haben, sind nicht bootfähig. Sie müssen die Datenträger zunächst anhängen und anschließend die Datei `.tgz` aus den Datenträgern kopieren. Die Methode zum Anhängen der DVD kann abhängig vom verwendeten Betriebssystem variieren.
- Die in den folgenden Beispielen verwendete Befehlssyntax kann abhängig vom verwendeten Betriebssystem variieren.
- Der PowerVM-Virtualisierungshypervisor erfordert 160 GB Plattenspeicherplatz. Empfohlen werden jedoch 500 GB Speicherplatz.
- Der PowerVM-Prozessor benötigt mindestens 1,0 Verarbeitungseinheiten und vier gemeinsam genutzte virtuelle Prozessoren mit begrenzter gemeinsamer Kapazitätsnutzung. Von der Verwendung dedizierter Prozessoren wird abgeraten. Der PowerVM-Prozessor erfordert zudem 16 GB Speicherplatz.

Zugehörige Informationen

HMC-V8-Netzinstallationsimages und -Installationsanweisungen

Virtuelle HMC-Appliance in x86-Umgebung installieren

Hier erfahren Sie, wie Sie die Virtuelle Hardware Management Console (HMC)-Appliance in einer x86-Umgebung installieren.

Virtuelle HMC-Appliance mit dem KVM-Hypervisor installieren

Hier erfahren Sie, wie Sie die Virtuelle Hardware Management Console (HMC)-Appliance mit dem Hypervisor für kernelbasierte virtuelle Maschinen (KVM-Hypervisor) installieren.

Führen Sie die folgenden Schritte aus, um die Virtuelle HMC-Appliance auf der KVM zu installieren:

Anmerkung: Bei den folgenden Schritten wird die Befehlszeilenschnittstelle verwendet. Zudem ist eine Rootberechtigung erforderlich. Die Befehlssyntax kann abhängig vom Betriebssystem variieren.

1. Überprüfen Sie, ob bei Systemen mit Red Hat Enterprise Linux (RHEL) ab Version 7.0 Virtualisierungspakete installiert sind.
2. Laden Sie die Datei <`Name der vHMC-Installationsdatei für KVM`>`.tar.gz` auf dem Hostsystem herunter.
3. Führen Sie folgenden Befehl aus: `mkdir -p /var/lib/libvirt/images/vHMC`.
4. Führen Sie folgenden Befehl aus: `cd /var/lib/libvirt/images/vHMC`.
5. Führen Sie den folgenden Befehl aus, um die virtuellen Plattenimages zu extrahieren: `tar -zxvf` <`Name der vHMC-Installationsdatei für KVM`>`.tgz`

   Anmerkung: Geben Sie in diesem Befehl den vollständigen Pfad der TAR-Datei Ihrer Virtuelle HMC-Appliance an.
6. In der Datei <`Name der vHMC-Installationsdatei für KVM`>`.tar.gz` wird die Datei **domain.xml** bereitgestellt. Führen Sie die folgenden Schritte aus:
   a. Bearbeiten Sie die Datei **domain.xml** und überprüfen Sie, ob der Pfad zu Ihren Platten richtig ist. Diese Datei enthält die Zeichenfolge **DISK_PATH**.
   b. Stellen Sie sicher, dass für den Buswert Ihrer Platteneinheit `virtio` verwendet wird.
   c. Sie können einen anderen Namen für Ihre VM auswählen. Der Standardname in der Datei **domain.xml** lautet **vHMC**.
   d. Überprüfen Sie, ob die MAC-Adresse (Media Access Control) in der Datei **domain.xml** festgelegt wurde. Diese Datei enthält die Zeichenfolge **MAC_ADDRESS**.

Anmerkung: Entfernen Sie diese Zeile, wenn automatisch eine MAC-Adresse für Sie generiert werden soll.

e. Überprüfen Sie, ob die Brücken mit Ihren Ethernet-Geräten übereinstimmen. In der Standarddatei **domain.xml** wird ein Ethernet angegeben.

f. Wenn Sie die Aktivierungsengine verwenden, dann ersetzen Sie **AEDISK** durch den Namen des virtuellen Plattenimage der Aktivierungsengine. Entfernen Sie andernfalls das Plattenelement.

7. Führen Sie den folgenden Befehl aus, um die VM zu definieren: `virsh define <Domäne>.xml`.
8. Führen Sie den folgenden Befehl aus, um zu prüfen, ob die virtuelle HMC zur Liste der definierten VMs hinzugefügt wurde: `virsh list --all`.
9. Führen Sie den folgenden Befehl aus, um die VM zu starten: `virsh start vHMC`.
10. Führen Sie den folgenden Befehl aus, um die Anzeigenummer für das Virtual Network Computing (VNC) Ihrer Konsole zu bestimmen: `virsh vncdisplay vHMC`.
11. Führen Sie den folgenden Befehl aus, um mit einer VNC-Anzeigefunktion eine Verbindung zu Ihrer Konsole herzustellen: `vncviewer HOSTNAME:ID`(Wobei "ID" für die Anzeigenummer steht, z. B. `0`).

    Anmerkung: Wenn Sie Remotezugriff benötigen, müssen Sie Ihre Firewall löschen oder sie so konfigurieren, dass ein Zugriff auf Port 5900 zulässig ist.

Virtuelle HMC-Appliance mit dem Xen-Hypervisor installieren

Hier erfahren Sie, wie Sie die Virtuelle Hardware Management Console (HMC)-Appliance mit dem Xen-Hypervisor installieren.

Die Virtuelle HMC-Appliance unterstützt Xen ab Version 4.2.

Führen Sie die folgenden Schritte aus, um die Virtuelle HMC-Appliance mit dem Xen-Hypervisor zu installieren:

Anmerkung: Bei den folgenden Schritten wird die Befehlszeilenschnittstelle verwendet. Zudem ist eine Rootberechtigung erforderlich. Die Befehlssyntax kann abhängig vom Betriebssystem variieren.

1. Überprüfen Sie, ob bei Systemen mit Red Hat Enterprise Linux (RHEL) ab Version 6.4 Virtualisierungspakete installiert sind.
2. Laden Sie die Datei `<Name der vHMC-Installationsdatei für XEN>.tar.gz` auf dem Hostsystem herunter.
3. Führen Sie folgenden Befehl aus: `mkdir -p /var/lib/libvirt/images/vHMC`.
4. Führen Sie folgenden Befehl aus: `cd /var/lib/libvirt/images/vHMC`.
5. Führen Sie den folgenden Befehl aus, um die virtuellen Plattenimages zu extrahieren: `tar -zxvf <Name der vHMC-Installationsdatei für Xen>.tgz`

   Anmerkung: Geben Sie in diesem Befehl den vollständigen Pfad der TAR-Datei Ihrer Virtuelle HMC-Appliance an.
6. In der Datei `<Name der vHMC-Installationsdatei für XEN>.tar.gz` wird die Datei **vhmc.cfg** bereitgestellt. Öffnen Sie die Datei **vhmc.cfg** in einem Texteditor und bearbeiten Sie folgende Werte:

   a. Ändern Sie den Wert der virtuellen HMC (optional): Bearbeiten Sie die Datei **vhmc.cfg** und überprüfen Sie, ob der Pfad zu Ihren Platten richtig ist. Diese Datei enthält die Zeichenfolge **DISK_PATH**.

   b. Ersetzen Sie **DISK_PATH** durch den Pfad für `disk1.img`:

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

   c. Ersetzen Sie **Ethernet-Adapter** und fügen Sie die MAC-Adresse hinzu (optional):

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

   Optionale MAC-Adresse:

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

Anmerkung: Wenn die virtuelle HMC neu gestartet wird, generiert der Xen-Hypervisor automatisch eine MAC-Adresse neu. Durch das Hinzufügen der optionalen MAC-Adresse wird dieses Problem behoben.

d. Ersetzen Sie **FLOPPYPATH** (wenn Sie die Aktivierungsengine verwenden):

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

7. Führen Sie den folgenden Befehl aus, um die VM zu erstellen und zu starten: `xl create vHMC.cfg`.
8. Führen Sie den folgenden Befehl aus, um zu prüfen, ob die VM zur Liste der definierten virtuellen Maschinen hinzugefügt wurde: `xl list`.
9. Führen Sie den folgenden Befehl aus, um auf die lokale VM-Konsole zuzugreifen: `vncviewer localhost 0`.

Virtuelle HMC-Appliance mit VMware ESXi installieren

Hier erfahren Sie, wie Sie die Virtuelle Hardware Management Console (HMC)-Appliance mit VMware ESXi installieren.

Sie können die Virtuelle HMC-Appliance auf VMware ESXi mit der grafischen Benutzerschnittstelle des vSphere-Clients installieren, damit die Open Virtualization Format(OVF)-Vorlage implementiert wird.

Anmerkung: Sie können die Virtuelle HMC-Appliance auf VMware ESXi ab Version 6.0 installieren.

Führen Sie die folgenden Schritte aus, um die Virtuelle HMC-Appliance mit dem vSphere-Client auf VMware ESXi zu installieren:

Anmerkung: Die Befehlssyntax kann abhängig vom Betriebssystem variieren.

1. Rufen Sie die TAR-Archivdatei ab: `<Name der vHMC-Installationsdatei für VMware>.tgz`.
2. Verwenden Sie den Befehl `tar`, um die OVA-Datei aus der TAR-Archivdatei zu extrahieren.
3. Starten Sie den vSphere-Client und melden Sie sich beim ESXi-Host an.
4. Wählen Sie über das Menü **Datei OVF-Vorlage implementieren** aus.
5. Klicken Sie auf **Durchsuchen** und wählen Sie die OVA-Datei aus.
6. Klicken Sie auf **Weiter**.
7. Klicken Sie nach Abschluss der Implementierung auf **Schließen** und wählen Sie das Virtuelle HMC-Appliance-Symbol zum Einschalten der Virtuelle HMC-Appliance aus.

Virtuelle HMC-Appliance auf POWER installieren

Hier erfahren Sie, wie Sie die Virtuelle Hardware Management Console (HMC)-Appliance in einer virtualisierten POWER-Umgebung installieren.

Virtuelle HMC-Appliance in PowerVM (logische Partition) installieren

Hier erfahren Sie, wie Sie die Virtuelle Hardware Management Console (HMC)-Appliance in einer PowerVM-Umgebung installieren.

Die Virtuelle HMC-Appliance unterstützt POWER9-Server in Firmwareversion FW910 oder höher. Weitere Informationen finden Sie unter Unterstützte Linux-Distributionen für POWER8 und POWER9 Linux on Power Systems (https://www.ibm.com/support/knowledgecenter/en/linuxonibm/liaam/liaamdistros.htm).

Notes:

1. Sie können den Server, auf dem sich die Virtuelle HMC-Appliance befindet, nicht verwalten.
2. Sie können den Server, auf dem sich eine andere Virtuelle HMC-Appliance befindet, nicht verwalten, wenn diese den Server verwaltet, auf dem sich diese Virtuelle HMC-Appliance befindet.

   Beispiel: Virtuelle HMC-Appliance A wird auf Server A ausgeführt und Virtuelle HMC-Appliance B auf Server B. Virtuelle HMC-Appliance A kann nicht Server B verwalten, während Virtuelle HMC-Appliance B zur gleichen Zeit Server A verwaltet. Eine der virtuellen HMC-Appliances kann den anderen Server

verwalten, beide virtuellen HMC-Appliances können jedoch nicht gleichzeitig den jeweils anderen Server verwalten.

.

Automatisiertes HMC-Installationsimage erstellen (optional)

Sie können ein automatisiertes HMC-Installationsimage erstellen, mit dem die Virtuelle HMC-Appliance automatisch installiert werden kann, ohne dass der **HMC-Installationsassistent** benötigt wird.

Anmerkung: Die Virtuelle HMC-Appliance auf PowerVM stellt keine Grafikadapterunterstützung für Adapter bereit, die der Partition zugeordnet sind. Sie können einen unterstützten Webbrowser verwenden, um eine Verbindung zur HMC für die Benutzerschnittstellenunterstützung herzustellen.

Führen Sie die folgenden Schritte aus, um ein automatisiertes HMC-Installationsimage zu erstellen:

1. Erstellen Sie zwei Verzeichnisse, indem Sie die folgenden Befehle ausführen: `mkdir -p oldiso` und `mkdir -p newiso`.
2. Hängen Sie das HMC-Installationsimage an das Verzeichnis **oldiso** an, indem Sie den folgenden Befehl ausführen: `sudo mount -o loop <image_path> oldiso`.
3. Kopieren Sie den Inhalt des Verzeichnisses **oldiso** in das Verzeichnis **newiso**, indem Sie den folgenden Befehl ausführen: `cp -r oldiso/* newiso`.
4. Bearbeiten Sie die Grub-Datei für die automatische Installation, indem Sie den folgenden Befehl ausführen: `sed -i 's/biosdevname=0/biosdevname=0 mode=auto optype=Install/' newiso/boot/grub/grub.cfg`.
5. Definieren Sie die Grub-Datei als schreibgeschützt, indem Sie den folgenden Befehl ausführen: `sudo chown 0444 newiso/boot/grub/grub.cfg`.
6. Erstellen Sie eine neue ISO-Datei für die HMC-Installation, indem Sie den folgenden Befehl ausführen: `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` (dabei muss **ISO label** als `HMC-<HMC-Version mit Releasenummer>` angegeben werden, zum Beispiel `HMC-8.0.870.0`).

Anmerkung: Weitere Informationen zum Einrichten der Aktivierungsengine und der Konfigurationsdatei finden Sie unter „Verwendung der Aktivierungsengine für die Virtuelle HMC-Appliance” auf Seite 32.

Einrichtung des logischen Datenträgers

Führen Sie die folgenden Schritte aus, um den logischen Datenträger einzurichten:

1. Wählen Sie ein verwaltetes System aus.
2. Wählen Sie im Menü-Pod **Systemaktionen** > **Power VM** > **Virtueller Speicher** aus.
3. Wählen Sie **System-VIOS verwalten** > **Aktion** > **Virtuellen Speicher verwalten** aus.
4. Wählen Sie die Registerkarte **Virtuelle Platten** aus.
5. Klicken Sie auf **Virtuelle Platte erstellen** und geben Sie die folgenden Informationen ein:
   - **Name der virtuellen Platte**: Der Name der virtuellen Platte.
   - **Speicherpoolname**: Der Name des Speicherpools.
   - **Größe der virtuellen Platte**: Die Größe der virtuellen Platte.
   - **Zugeordnete Partition**: Der Name der logischen Partition.

   Anmerkung: Es ist ein Plattenspeicherplatz von mindestens 160 GB erforderlich (500 GB Plattenspeicherplatz wird empfohlen).

Einrichtung des Installationsmediums - Datenträgerbibliothek erstellen

Führen Sie die folgenden Schritte aus, um eine Datenträgerbibliothek zu erstellen:

1. Wählen Sie ein verwaltetes System aus.
2. Wählen Sie im Menü-Pod **Systemaktionen** > **Power VM** > **Virtueller Speicher** aus.
3. Wählen Sie **System-VIOS verwalten** > **Aktion** > **Virtuellen Speicher verwalten** aus.
4. Wählen Sie die Registerkarte **Optische Einheiten** aus.
5. Klicken Sie auf **Bibliothek erstellen** und geben Sie die folgenden Informationen ein:
   - **Speicherpool**: Der Name des Speicherpools.
   - **Größe der Datenträgerbibliothek**: Die Größe der Datenträgerbibliothek.
6. Klicken Sie auf **OK**.

Einrichtung des Installationsmediums - Datenträger an VIOS hochladen

Führen Sie die folgenden Schritte aus, um Datenträger an den virtuellen E/A-Server (Virtual I/O Server, VIOS) hochzuladen:

1. Melden Sie sich beim VIOS an.
2. Führen Sie im VIOS-Rootmodus den folgenden Befehl aus: `oem_setup_env`.
3. Führen Sie den folgenden Befehl aus, um eine NFS-Verbindung zu ermöglichen: `nfso -o nfs_use_reserved_ports=1`.
4. Führen Sie den folgenden Befehl aus, um das NFS an den lokalen VIOS-Ordner anzuhängen: `mount <server_ip>:/Mountpoint <local_folder>`.
5. Führen Sie den folgenden Befehl aus, um zu überprüfen, ob der NFS-Mount Ihre ISO-Datei für die HMC-Installation und das Image für die Konfiguration der Aktivierungsengine enthält (optional): `ls`.

Einrichtung des Installationsmediums - Datenträger mit Datenträgerbibliothek verknüpfen

Führen Sie die folgenden Schritte aus, um den Datenträger mit der Datenträgerbibliothek zu verknüpfen:

1. Navigieren Sie zurück zu **System-VIOS verwalten** > **Aktion** > **Virtuellen Speicher verwalten** und wählen Sie die Registerkarte **Optische Einheiten** aus.
2. Wählen Sie im Abschnitt **Virtuelle optische Medien** die Option **Datenträger hinzufügen** im Menü **Aktionen** aus.
3. Wählen Sie im Fenster **Hinzufügen virtueller Datenträger** die Option **Hinzufügen einer vorhandenen Datei von VIOS-Dateisystem** aus und geben Sie die folgenden Informationen ein:
   - **Datenträgername**: Der Name des Datenträgers (zum Beispiel `HMCInstall` oder `AEDrive`).
   - **Name der optischen Datenträgerdatei**: Der Dateiname der ISO-Datei für die Installation (zum Beispiel `01234567-ppc64ie.iso`).
4. Klicken Sie auf **OK**.
5. Wenn Sie ein Image für die Konfiguration der Aktivierungsengine erstellt haben, dann wiederholen Sie die Schritte 3 - 4, um Image für die Konfiguration der Aktivierungsengine hinzuzufügen. Fahren Sie andernfalls mit Schritt 6 fort.
6. Überprüfen Sie, ob das optische Medium in die Datenträgerbibliothek hochgeladen wurde. Dazu müssen Sie überprüfen, ob der Datenträgername in der Liste der verfügbaren **virtuellen optischen Medien** angezeigt wird.

Einrichtung der logischen Partition

Führen Sie die folgenden Schritte aus, um die logische Partition einzurichten:

1. Wählen Sie ein verwaltetes System aus.
2. Wählen Sie im Menü-Pod **Systemaktionen** > **Partitionen** > **Partitionen** aus.
3. Klicken Sie auf **Partition erstellen** und geben Sie die folgenden Informationen ein:

- **Partitionsname**: Der Name der Partition.
- **Partitions-ID**: Die ID der Partition.
- **Partitionstyp**: Wählen Sie das Betriebssystem aus (**AIX/Linux** oder **IBM i**).

4. Klicken Sie auf **OK**.
5. Ordnen Sie die Anzahl der Prozessoren und die Speicherkapazität für die Partition zu.

   Anmerkung: Es sind mindestens vier virtuelle Prozessoren und 8 GB Speicher erforderlich.
6. Wählen Sie im Menü-Pod **Partitionsaktionen** > **Virtuelle E/A** > **Virtuelle Netze** aus.
7. Klicken Sie auf **Virtuelles Netz anhängen** und aktivieren Sie das Kontrollkästchen **Neue virtuelle Ethernet-Adapter anzeigen und anschließen**. Wählen Sie aus der Tabelle die virtuellen Netzadapter aus, die Sie an die logische Partition anschließen möchten.

   Anmerkung: Es sind maximal vier virtuelle Netzadapter zulässig.
8. Wählen Sie im Menü-Pod **Partitionsaktionen** > **Virtuelle E/A** > **Virtueller Speicher** aus.
9. Klicken Sie auf der Registerkarte **Virtuelle optische Einheit** auf **Virtuelle optische Einheit hinzufügen**.
10. Geben Sie den **Einheitennamen** (z. B. `HMCInstall` oder `AEDrive`) ein und wählen Sie den gewünschten virtuellen E/A-Server in der Tabelle aus.

    Anmerkung: Die Installation von `AEDrive` ist optional.
11. Klicken Sie auf **OK**.
12. Überprüfen Sie, ob die virtuellen optischen Einheiten, die Sie in Schritt 10 hinzugefügt haben, jetzt in der Tabelle aufgelistet sind.
13. Klicken Sie im Menü **Aktion** auf **Laden**.
14. Wählen Sie die Datenträgerdatei aus, die der logischen Partition zugeordnet werden soll, und klicken Sie auf **OK**.
15. Überprüfen Sie, ob die virtuellen optischen Einheiten, die Sie in Schritt 13 geladen haben, jetzt in der Tabelle aufgelistet sind.

Virtuelle HMC-Appliance starten

Anmerkung: Wenn Sie die Virtuelle HMC-Appliance auf einer Partition mit der ISO-Imagedatei der HMC installieren, haben Sie mit der lokalen grafischen Konsole keinen Zugriff auf die Webbenutzerschnittstelle.

Führen Sie die folgenden Schritte aus, um die Virtuelle HMC-Appliance auf PowerVM zu starten:

1. Wählen Sie die verwaltete Partition aus.
2. Öffnen Sie eine aktive Verbindung zur logischen Partition, indem Sie **Aktionen** > **Konsole** > **Terminalfenster öffnen** auswählen.
3. Aktivieren Sie die logische Partition, indem Sie **Aktionen** > **Aktivieren** auswählen.
4. Wählen Sie **Aktivieren (Normal)** und **Aktuelle Konfiguration** aus.
5. Klicken Sie auf **Fertig stellen**.
6. Wechseln Sie zum Terminalfenster.
7. Wählen Sie im **Boot**-Menü die Option **1 = SMS-Menü** aus.
8. Wählen Sie im **Haupt**-Menü die Option **5 = Bootoptionen auswählen** aus.
9. Wählen Sie im **Multiboot**-Menü die Option **1 = Einheit installieren/booten** aus.
10. Wählen Sie im Menü **Einheitentyp auswählen** die Option **5 = Alle Einheiten auflisten** aus.
11. Wählen Sie die Einheit `HMCInstall` entsprechend der Einheitenposition aus.
12. Wählen Sie **2. Booten im normalen Modus** aus.
13. Wählen Sie **1. Ja** aus, um dies zu bestätigen.
14. Befolgen Sie die Anweisungen im **HMC-Installationsassistenten**.

Anmerkung: Überspringen Sie diesen Schritt, wenn Sie ein automatisiertes HMC-Installationsimage verwendet haben.

15. Nach Abschluss der Installation und dem Starten des Systems müssen Sie im Dialogfeld **Sprachauswahl** eine Sprache auswählen.
16. Akzeptieren Sie die Lizenzvereinbarung.

    Anmerkung: Stellen Sie vor der Ausführung eines Befehls sicher, dass der Befehlscontroller bereit ist, Befehle anzunehmen. Beispiel: Die Ausführung des Befehls **lshmc -V**, bis sie erfolgreich umgesetzt wurde.
17. Melden Sie sich als `hscroot` an und verwenden Sie den Befehl **chhmc** für die Konfiguration des Netzes.

    Im folgenden Beispiel wird die Folge der **chhmc**-Befehle dargestellt, die für die Konfiguration des Netzes und die Aktivierung von SSH-Zugriff (Secure Shell) und Webfernzugriff auf der HMC verwendet werden können.

    ```
    chhmc -c network -s modify -i ethX -a <IP-Adresse der HMC> -nm <Netzmaske der HMC> --lpar
    comm on
    chhmc -c network -s modify -h <Hostname der HMC> -d <Domänenname der HMC> -g <Gateway-IP>
    chhmc -c network -s add -ns <Name-Server> -ds <Domänensuche>
    chhmc -c ssh -s enable
    chhmc -c ssh.name -s add -a <IP-Adresse>
    chhmc -c SecureRemoteAccess.name -s add -a <IP-Adresse>
    chhmc -c remotewebui -s enable -i ethX
    hmcshutdown -r -t now
    ```

    - **ethX** ist der Name der Netzschnittstelle, die konfiguriert werden soll.
    - **IP-Adresse der HMC** steht für die IP-Adresse Ihrer HMC.
    - **Netzmaske der HMC** steht für die Netzmaske Ihrer HMC.
    - **Hostname der HMC** steht für den Hostnamen Ihrer HMC.
    - **Domänenname der HMC** steht für den Domänennamen Ihrer HMC.
    - **Gateway-IP** steht für die IP-Adresse des Gateways in Ihrem Netz.
    - **Name-Server** steht für die Name-Server-Adresse Ihres Netzes.
    - **Domänensuche** steht für die Namen der Domänen, die von der HMC durchsucht werden sollen.
    - Verwenden Sie **-a 0.0.0.0 -nm 0** anstelle von **IP-Adresse**, um Zugriff auf alle IP-Adressen zuzulassen.

    Anmerkung: Wenn Sie mehrere virtuelle Ethernet-Adapter verwenden, führen Sie in den einzelnen Schnittstellen den Befehl **cat/etc/sysconfig/network-scripts/ifcfg-ethX** auf der virtuellen HMC-Appliance aus. Vergleichen Sie die MAC-Adresse (Media Access Control) mit der Angabe durch die HMC in der Adapteransicht des virtuellen Netzes der Partition. Wenn Sie auf **Einstellungen für virtuellen Ethernet-Adapter anzeigen** klicken, erhalten Sie weitere Informationen zu den virtuellen Ethernet-Adaptern. Mit diesem Schritt können Sie ermitteln, welche Schnittstelle verwendet werden muss.
18. Starten Sie das System neu.

Verwendung der Aktivierungsengine für die Virtuelle HMC-Appliance

Hier erfahren Sie, wie Sie die Aktivierungsengine für die Virtuelle Hardware Management Console (HMC)-Appliance verwenden.

Die Aktivierungsengine ist ein Framework, mit dem verschiedene Komponenten innerhalb einer virtuellen Maschine während eines Systemstarts konfiguriert werden können. Für die Verwendung der Aktivierungsengine müssen Sie ein XML-Konfigurationsprofil einrichten, damit sich die Virtuelle HMC-Appliance beim ersten Start in einem Status befindet, in dem sie für die Verwaltung bereit ist. Weitere Informationen zur Konfiguration des XML-Konfigurationsprofils finden Sie unter „Konfigurationsprofil für die Aktivierungsengine einrichten" auf Seite 33. Die Konfigurationsdatei kann für die Konfiguration der folgenden Optionen verwendet werden:

- Einstellung der Standardtastatur (US)
- Standardländereinstellung (US)
- Inaktivierung der Tastaturkonfiguration
- Inaktivierung der Bildschirmdefinition
- Lizenzvereinbarung und Maschinencodevereinbarung
- Inaktivierung des Installationsassistenten
- Inaktivierung des Assistenten für die Call-Home-Funktion
- Konfiguration von bis zu vier Netzschnittstellenkarten
- Konfiguration von Firewalleinstellungen für die einzelnen Schnittstellen
- Konfiguration der Netzschnittstelle als IPv4-DHCP-Server
- Konfiguration der privaten und der offenen Schnittstelle
- Konfiguration der Standardgateway-Schnittstelleneinheit

Anmerkung: Die Anzahl der Ethernet-Adapter, die in der Konfigurationsdatei **vHMC-Conf.xml** definiert ist, muss mit den definierten Netzadaptern in der Konfigurationsdatei **domain.xml**, **vHMC.cfg** oder **VMWare** korrelieren.

Für die Aktivierungsengine ist eine virtuelle Platte erforderlich, die eine XML-Konfiguration enthält. Sie können die Datei **user_data** mit einem Texteditor bearbeiten und das folgende Beispiel als Leitfaden für die XML-Konfiguration verwenden.

Führen Sie die folgenden Schritte aus, um ein virtuelles ISO-Plattenimage mit Aktivierungsengine-Konfiguration in einer Linux-Umgebung zu erstellen:

1. Erstellen Sie ein Verzeichnis:

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

2. Kopieren Sie die bearbeitete Datei **user_data** in das Verzeichnis:

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

3. Erstellen Sie ein virtuelles Plattenimage mit der Aktivierungsengine-Konfiguration:

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

Konfigurationsprofil für die Aktivierungsengine einrichten

Hier erfahren Sie, wie Sie mithilfe von XML-Tags die Konfigurationsdatei für die Aktivierungsengine einrichten.

Konfigurationsdatei

Das folgende Beispiel der Konfigurationsdatei können Sie verwenden, um die XML-Tags besser zu verstehen.

```
<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>
```

XML-Tags für die Konfigurationsdatei

XML-Tags werden in der Konfigurationsdatei für die Aktivierungsengine verwendet, um bestimmte Werte für verschiedene Attribute einzurichten. Sie können diese Werte in der Konfigurationsdatei für die Aktivierungsengine manuell festlegen. In der folgenden Tabelle finden Sie eine Beschreibung der einzelnen Tags und der zugehörigen zulässigen Werte:

Tabelle 9. XML-Tags

Tags	Beschreibung	Zulässige Werte	Notes
ConfigurationVersion	Erforderliches Element zum Definieren der zu verwendenden Konfigurationsversion.	**2.0**	
LicenseAgreement	Erforderliches Element zum Anzeigen der Virtuelle HMC-Appliance-Lizenzvereinbarung.		
AcceptLicense	Erforderliches Element zum Akzeptieren der Virtuelle HMC-Appliance-Lizenzvereinbarung.	• **Yes**: Akzeptiert die HMC-Lizenzvereinbarung. • **No**: Fordert Benutzer auf, die HMC-Lizenzvereinbarung zu akzeptieren.	Wenn ein ungültiger Wert eingegeben wird, verwendet die Aktivierungsengine die Standardeinstellung **No**.
Locale	Erforderliches Element zum Definieren der Ländereinstellungen.	**en_US.UTF-8**	Wenn ein ungültiger Wert eingegeben wird, verwendet die Aktivierungsengine die Standardeinstellung **US**.

Tabelle 9. XML-Tags (Forts.)

Tags	Beschreibung	Zulässige Werte	Notes
SetupWizard	Erforderliches Element zum Aktivieren oder Inaktivieren des **HMC-Installationsassistenten**.	• **Yes**: Zeigt den **HMC-Installationsassistenten** an. • **No**: Inaktiviert die Anzeige des **HMC-Installationsassistenten**.	Wenn ein ungültiger Wert eingegeben wird, verwendet die Aktivierungsengine die Standardeinstellung **Yes**.
SetupCallHomeWizard	Erforderliches Element zum Aktivieren oder Inaktivieren des **HMC-Assistenten zur Einrichtung der Call-Home-Funktion**.	• **Yes**: Zeigt den **HMC-Assistenten zur Einrichtung der Call-Home-Funktion** an. • **No**: Inaktiviert die Anzeige des **HMC-Assistenten zur Einrichtung der Call-Home-Funktion**.	Wenn ein ungültiger Wert eingegeben wird, verwendet die Aktivierungsengine die Standardeinstellung **Yes**.
SetupKeyboard	Erforderliches Element zum Definieren der Tastaturkonfiguration.	• **Yes**: Fordert den Benutzer zur Tastaturkonfiguration auf. • **No**: Akzeptiert die Standardtastaturkonfiguration (US).	Wenn ein ungültiger Wert eingegeben wird, verwendet die Aktivierungsengine die Standardeinstellung **Yes**.
SetupDisplay	Erforderliches Element zum Aktivieren oder Inaktivieren der Anzeigekonfiguration.	• **Yes**: Fordert den Benutzer zur Anzeigekonfiguration auf. • **No**: Akzeptiert die Standardanzeigekonfiguration.	Wenn ein ungültiger Wert eingegeben wird, verwendet die Aktivierungsengine die Standardeinstellung **Yes**.
Ethernet	Erforderliches Element, das Werte für Ethernet-Adapterkonfigurationen enthält. Es können maximal vier Ethernet-Adapter konfiguriert werden.	**Enable**: • **Yes**: Diesen Adapter konfigurieren. • **No**: Diesen Adapter nicht konfigurieren. **DefaultGatewayDevice**: • **Yes**: Diesen Adapter als Hauptnetzadapter konfigurieren. • **No**: Diesen Adapter nicht als Hauptnetzadapter konfigurieren. **PrivateInterface**: • **Yes**: Diesen Adapter als private Schnittstelle konfigurieren. **Yes** ist erforderlich, um die Schnittstelle als IPv4-DHCP-Server zu konfigurieren. • **No**: Diesen Adapter nicht als private Schnittstelle konfigurieren. **No** ist erforderlich, um die Schnittstelle als statische IPv4-Schnittstelle zu konfigurieren.	Wenn im Abschnitt zum Ethernet-Adapter ungültige Werte eingegeben wurden oder wenn mit **DefaultGatewayDevice** mehrere Standardgateway-Einheiten definiert wurden, führt die Aktivierungsengine die Standardkonfiguration aus. Optionale Elemente können in der Konfiguration weggelassen werden. Es ist mindestens eine IPV4- oder IPV6-Konfiguration erforderlich. Wenn Sie keine IP-Konfiguration angeben, verwendet die Aktivierungsengine die Standardkonfiguration.

Tabelle 9. XML-Tags (Forts.)

Tags	Beschreibung	Zulässige Werte	Notes
HostName	Optionales Element zum Definieren des Namens des Netzhosts.	Eine beliebige gültige Zeichenfolge für den Hostnamen.	Wenn das Element nicht definiert ist, verwendet die Aktivierungsengine als Standardwert für **HostName** den lokalen Host.
Domain	Optionales Element zum Definieren der Netzdomäne.	Ein beliebiger gültiger Domänenwert (zum Beispiel **example.us.com**).	Wenn das Element nicht definiert ist, verwendet die Aktivierungsengine als Standardwert für **Domain** einen leeren Wert.
DNSServers	Optionales Element zum Definieren der Netz-DNS-Server.	Es ist zulässig, als DNS-Server einen Wert oder bis zu drei gültige IPv4- oder IPv6-Adressen, die durch ein Komma voneinander getrennt sind, zu verwenden. • Beispiel 1: IPv4: 8.3.2.1 IPv6: 2001:4860:4860::8888 • Beispiel 2: IPv4: 8.3.2.1,8.5.4.1 IPv6: 2001:4860:4860::8888,2001:4860:4860::8844 • Beispiel 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	Wenn das Element nicht definiert ist, verwendet die Aktivierungsengine als Standardwert für **DNSServers** einen leeren Wert.

Tabelle 9. XML-Tags (Forts.)

Tags	Beschreibung	Zulässige Werte	Notes
IP4Config	Optionales Element zum Definieren der IPv4-Konfigurationseinstellungen.	**IPType**: Erforderliches Element zum Definieren des Typs der IPv4-Konfiguration. • **Static**: Diesen Adapter mit statischer Konfiguration konfigurieren. • **DHCP**: Diesen Adapter mit DHCP-Konfiguration konfigurieren. • **DHCPServer**: Diesen Adapter als IPv4-DHCP-Server konfigurieren (dabei muss **PrivateInterface** auf **Yes** festgelegt sein). **IPAddress**: Optionales Element, das nur erforderlich ist, wenn die Konfiguration **Static** oder **DHCPServer** ausgewählt wurde. • **Static Configuration**: Beliebiger gültiger Wert für die IPv4-Adresse. • **DHCPServer Configuration**: Beliebige DHCP-Server-IP im IP-Bereich. **Netmask**: Optionales Element, das nur erforderlich ist, wenn die Konfiguration **Static** ausgewählt wurde. • Beliebiger gültiger Wert für die IPv4-Netzmaske. **Gateway**: Optionales Element, das nur erforderlich ist, wenn die Konfiguration **Static** ausgewählt wurde. • Beliebiger gültiger Wert für die IPv4-Netzmaske.	
IP6Config	Optionales Element zum Definieren der IPv6-Konfigurationseinstellungen.	**IPType**: Erforderliches Element zum Definieren des Typs der IPv6-Konfiguration. • **Static**: Diesen Adapter mit statischer Konfiguration konfigurieren. • **DHCP**: Diesen Adapter mit DHCP-Konfiguration konfigurieren. **IPAddress**: Es ist zulässig, IPv6-Format und IPv6-Präfix jeweils in Lang- oder Kurzform anzugeben. • Beispiel 1: IPv6: 2001:4860:4860:0000:0000:0000:0000:8888 • Beispiel 2: IPv6: 2001:4860:4860::8888 • Beispiel 3: IPv6: 2001:4860:4860::8888/128 Wenn kein Präfix eingegeben wird, verwendet die Aktivierungsengine als Standardeinstellung das Präfix /64. **Gateway**: • Beliebiger gültiger Wert für die IPv6-Adresse.	

Tabelle 9. XML-Tags (Forts.)

Tags	Beschreibung	Zulässige Werte	Notes
Firewall	Optionales Element zum Definieren der Firewalleinstellungen.	**PEGASUS**: • **Enabled**: Lässt zu, dass die PEGASUS-Ports geöffnet sind. • **Disabled**: Inaktiviert die PEGASUS-Ports. **RPD**: • **Enabled**: Lässt zu, dass die RMC-Ports geöffnet sind. • **Disabled**: Inaktiviert die RMC-Ports. **FCS**: • **Enabled**: Lässt zu, dass die FCS-Ports geöffnet sind. • **Disabled**: Inaktiviert die FCS-Ports. **I5250**: • **Enabled**: Lässt zu, dass die 5250-Ports geöffnet sind. • **Disabled**: Inaktiviert die 5250-Ports. **PING**: • **Enabled**: Lässt zu, dass der 5250-Port geöffnet ist. • **Disabled**: Inaktiviert den Ping-Port. **L2TP**: • **Enabled**: Lässt zu, dass die L2TP-Ports geöffnet sind. • **Disabled**: Inaktiviert die L2TP-Ports. **SLP**: • **Enabled**: Lässt zu, dass die SLP-Ports geöffnet sind. • **Disabled**: Inaktiviert die SLP-Ports. **RSCT**: • **Enabled**: Lässt zu, dass die RSCT-Ports geöffnet sind. • **Disabled**: Inaktiviert die RSCT-Ports. **SECUREREMOTEACCESS**: • **Enabled**: Lässt zu, dass die Ports für den sicheren Remotezugriff geöffnet sind. • **Disabled**: Inaktiviert die Ports für den sicheren Remotezugriff. **SSH**: • **Enabled**: Lässt zu, dass der SSH-Port geöffnet ist. • **Disabled**: Inaktiviert den SSH-Port.	

Tabelle 9. XML-Tags (Forts.)

Tags	Beschreibung	Zulässige Werte	Notes
Firewall	Optionales Element zum Definieren der Firewalleinstellungen.	**NTP**: • **Enabled**: Lässt zu, dass die NTP-Ports geöffnet sind. • **Disabled**: Inaktiviert die NTP-Ports. **SMNPTraps**: • **Enabled**: Lässt zu, dass die Ports für SMNP-Traps geöffnet sind. • **Disabled**: Inaktiviert die Ports für SMNP-Traps. **SMNPAgents**: • **Enabled**: Lässt zu, dass die Ports für SMNP-Agenten geöffnet sind. • **Disabled**: Inaktiviert die Ports für SMNP-Agenten.	

NTPServers	Der Tag **NTPServers** ist erforderlich, wenn Sie bis zu fünf NTP-Server in einer Virtuelle HMC-Appliance konfigurieren möchten.	**NTPServers**: Akzeptiert `<ntpparam ntpserver="server" ntpversion="version"/>`
		ntpparam:
		• **ntpserver**: Akzeptiert beliebige gültige IPv4- oder IPv6-Werte und gültige Hostnamen.
		• **ntpversion**: Akzeptiert den numerischen Wert `1-4`.
		Beispiel:
		`<NTPServers>`
		`  <ntpparam ntpserver="test.aus tin.ibm.com" ntpversion="2"/>`
		`  <ntpparam ntpser ver="192.168.34.1"`
		`  ntpversion="4"/>`
		`  <ntpparam ntpser ver="::ffff:903:201"`
		`  ntpversion="3"/>`
		`</NTPServers>`	

HMC konfigurieren

Hier wird beschrieben, wie Sie Ihre Netzverbindungen einrichten, Ihre HMC konfigurieren, Schritte nach der Konfiguration ausführen sowie Ihre HMC aktualisieren und Upgrades für Ihre HMC durchführen.

Netzeinstellungen auf der HMC auswählen

Dieser Abschnitt informiert Sie über die Netzeinstellungen, die Sie für die Hardware Management Console (HMC) verwenden können.

HMC-Netzverbindungen

Hier erfahren Sie, wie die Hardware Management Console (HMC) in einem Netz verwendet werden kann.

Sie können verschiedene Arten von Netzverbindungen verwenden, um Ihre HMC mit verwalteten Systemen zu verbinden. Weitere Informationen zum Konfigurieren der HMC für die Verbindung mit einem Netz finden Sie unter „HMC konfigurieren” auf Seite 56. Weitere Informationen zum Verwenden der HMC in einem Netz finden Sie in den folgenden Abschnitten:

Arten von HMC-Netzverbindungen

Hier erfahren Sie, wie Sie die Fernverwaltungs- und Servicefunktionen der HMC mit Ihrem Netz verwenden.

Die HMC unterstützt die folgenden Arten einer logischen Kommunikation:

HMC zu verwaltetem System
Diese Art der Kommunikation wird verwendet, um den Großteil der Hardwaremanagementfunktionen auszuführen, bei denen die HMC Steuerfunktionsanforderungen über den Serviceprozessor des verwalteten Systems ausgibt. Die Verbindung zwischen der HMC und dem Serviceprozessor wird gelegentlich als *Servicenetz* bezeichnet. Diese Verbindung ist für die Verwaltung von verwalteten Systemen erforderlich.

HMC zu logischer Partition
Wird zur Erfassung plattformbezogener Informationen (Hardwarefehlerereignisse, Hardwareinventar) von den Betriebssystemen verwendet, die auf den logischen Partitionen ausgeführt werden, sowie zur Koordination bestimmter Plattformaktivitäten (dynamisches LPAR, Reparatur bei eingeschalteter Einheit) mit diesen Betriebssystemen. Wenn Sie die Funktionen zu Service- und Fehlerhinweisen verwenden möchten, müssen Sie diese Verbindung herstellen.

HMC mit BMC

Anmerkung: Die Baseboard-Management-Controller(BMC)-Verbindung ist nur für Modell 7063-CR1 der HMC gültig.

Sie wird für die Durchführung von Service- und Wartungstasks verwendet. Die BMC-Verbindung wird verwendet, um die HMC-Firmware auf dem System zu laden und zu warten. Diese Verbindung ist für den Zugriff auf den BMC auf der HMC erforderlich.

HMC zu fernen Benutzern
Diese Art der Kommunikation stellt fernen Benutzern Zugriff auf die HMC-Funktionen bereit. Ferne Benutzer können auf folgende Arten auf die HMC zugreifen:

- Mithilfe des Web-Browsers, um über Remotezugriff auf alle Funktionen der HMC-GUI zuzugreifen.
- Mit SSH (Secure Socket Shell), um über Remotezugriff auf die HMC-Befehlszeilenfunktionen zuzugreifen.
- Mit einem virtuellen Terminalserver, um über Remotezugriff auf virtuelle logische Partitionskonsolen zuzugreifen.

HMC zu Service und Support
Diese Art der Kommunikation wird zum Übertragen von Daten (z. B. Hardwarefehlerberichte, Bestandsdaten und Mikrocodeaktualisierungen) zum und vom Service-Provider verwendet. Sie können diesen Kommunikationspfad für automatische Serviceaufrufe verwenden.

Die HMC kann, abhängig vom Modell, bis zu vier separate physische Ethernet-Schnittstellen unterstützen. Die Standalone-Version der HMC unterstützt nur drei HMC-Schnittstellen, die einen integrierten Ethernet-Adapter und bis zu zwei Plug-in-Adapter verwenden. Verwenden Sie die einzelnen Schnittstellen wie folgt:

- Eine Netzschnittstelle kann ausschließlich für die Kommunikation zwischen HMC und verwaltetem System verwendet werden. Dies bedeutet, dass sich nur die HMC und die Serviceprozessoren des verwalteten Systems in diesem Netz befinden. Mindestens eine Netzschnittstelle kann ausschließlich für die Kommunikation zwischen HMC und verwaltetem System verwendet werden. Dies bedeutet, dass sich nur die HMC und die Serviceprozessoren des verwalteten Systems in diesem Netz befinden. Auch wenn die Netzschnittstellen der Serviceprozessoren für das SSL-Protokoll (Secure Sockets Layer) verschlüsselt und kennwortgeschützt sind, kann ein separat dediziertes Netz zu einer verbesserten Sicherheit dieser Schnittstellen beitragen.
- In der Regel wird eine offene Netzschnittstelle für die Netzverbindung zwischen der HMC und den logischen Partitionen auf den verwalteten Systemen, d. h. für die Kommunikation zwischen der HMC und den logischen Partitionen, verwendet. Mit dieser offenen Netzschnittstelle können Sie die HMC auch über Remotezugriff verwalten.

- Wahlweise können Sie auch eine dritte Schnittstelle verwenden, um eine Verbindung zu logischen Partitionen herzustellen und um die HMC über Remotezugriff zu verwalten. Diese Schnittstelle kann auch als separate HMC-Verbindung zu verschiedenen Gruppen logischer Partitionen verwendet werden. Dies ist z. B. der Fall, wenn Sie über ein Verwaltungs-LAN verfügen möchten, das von dem LAN getrennt ist, auf dem die üblichen Geschäftstransaktionen aktiv sind. Ferne Administratoren können mit dieser Methode auf die HMC und andere verwaltete Einheiten zugreifen. Manchmal befinden sich die logischen Partitionen in verschiedenen Netzsicherheitsdomänen - möglicherweise hinter einer Firewall -, und in jeder der beiden Domänen sollen verschiedene HMC-Netzverbindungen vorhanden sein.

Anforderungen an die Web-Browser für HMC

Die Hardware Management Console (HMC) Version 9.1.0 wird von Google Version 57, Microsoft Internet Explorer (IE) Version 11.0, Mozilla Firefox Version 45 und 52 Extended Support Release (ESR) und Safari Version 10.1 unterstützt.

Wenn Ihr Browser für die Verwendung eines Internet-Proxys konfiguriert ist, sollte eine lokale IP-Adresse in der Ausnahmeliste enthalten sein. Weitere Informationen zur Ausnahmeliste erhalten Sie von Ihrem Netzadministrator. Wenn Sie trotzdem den Proxy für den Zugang zur HMC verwenden möchten, aktivieren Sie in Ihrem Fenster "Internetoptionen" auf der Registerkarte "Erweitert" die Option "HTTP 1.1 über Proxyverbindungen verwenden".

Damit ASMI funktioniert, wenn die Verbindung zur HMC über Fernzugriff hergestellt wird, müssen Sitzungscookies aktiviert werden. Der ASM-Proxy-Code speichert Sitzungsdaten und verwendet sie. Führen Sie die Schritte zum Aktivieren der Sitzungscookies aus.

Aktivieren der Sitzungscookies in Internet Explorer.

1. Wählen Sie "Extras" aus und klicken Sie auf "Internetoptionen".
2. Wählen Sie "Datenschutz" aus und klicken Sie auf "Erweitert".
3. Überprüfen Sie, ob "Sitzungscookies immer zulassen" aktiviert ist. Ist dies nicht der Fall, wählen Sie "Automatische Cookiebehandlung außer Kraft setzen" und dann "Sitzungscookies immer zulassen" aus.
4. Wählen Sie "Bestätigen" unter "Cookies von Erstanbietern" und unter "Cookies von Drittanbietern" aus.
5. Klicken Sie auf "OK".

Aktivieren der Sitzungscookies in Firefox.

1. Wählen Sie "Extras" aus und klicken Sie auf "Optionen".
2. Klicken Sie auf "Cookies".
3. Wählen Sie aus, dass Sites Cookies festlegen dürfen.
4. Wählen Sie "Ausnahmen" aus und fügen Sie HMC hinzu.
5. Klicken Sie auf "OK".

Private und offene Netze in der HMC-Umgebung
Die Hardware Management Console (HMC) kann für die Verwendung von offenen und privaten Netzen konfiguriert werden. Bei privaten Netzen kann ein bestimmter Bereich von nicht weiterleitbaren IP-Adressen verwendet werden. Ein *öffentliches* oder "offenes" Netz bezeichnet eine Netzverbindung zwischen der HMC und logischen Partitionen sowie anderen Systemen in Ihrem regulären Netz.

Private Netze

Die einzigen Einheiten im privaten Netz der HMC sind die HMC selbst und jedes verwaltete System, an das die HMC angeschlossen ist. Die HMC ist mit dem flexiblen Serviceprozessor (Flexible Service Processor, FSP) jedes verwalteten Systems verbunden.

Bei den meisten Systemen weist der FSP zwei Ethernet-Anschlüsse mit der Bezeichnung **HMC1** und **HMC2** auf. Dadurch können Sie bis zu zwei HMCs anschließen.

Einige Systeme verfügen über zwei FSPs. In einem solchen Fall fungiert der zweite FSP als redundantes Backup. Die Voraussetzungen bei der Basisinstallation sind für ein System mit zwei FSPs im Wesentlichen dieselben wie für ein System ohne einen zweiten FSP. Die HMC muss mit jedem FSP verbunden sein. Aus diesem Grund ist zusätzliche Netzhardware erforderlich (zum Beispiel ein LAN-Switch oder ein Hub), wenn mehrere FSPs oder mehrere verwaltete Systeme vorhanden sind.

Anmerkung: Pro FSP-Anschluss auf dem verwalteten System darf nur eine HMC angeschlossen sein.

Öffentliche Netze

Bei dem offenen bzw. öffentlichen Netz kann die Internetverbindung über eine Firewall oder einen Router erfolgen. Die Verbindung mit dem Internet ermöglicht der HMC, die Call-Home-Funktion zu nutzen, wenn Hardwarefehler gemeldet werden müssen.

Die HMC selbst stellt ihre eigene Firewall für jede ihrer Netzschnittstellen bereit. Wenn der Assistent zur Installationsanleitung (Guided Setup Wizard) der HMC ausgeführt wird, wird dabei automatisch eine einfache Firewall konfiguriert. Nachdem die Erstinstallation/-konfiguration der HMC abgeschlossen ist, werden jedoch die Firewall-Einstellungen angepasst.

HMC als DHCP-Server
Sie können die Hardware Management Console (HMC) als DHCP-Server (DHCP = Dynamic Host Configuration Protocol) verwenden.

Wenn Sie die erste Netzschnittstelle als privates Netz konfigurieren möchten, können Sie für den DHCP-Server eine Auswahl aus einem Bereich von IP-Adressen treffen, die er seinen Clients zuweisen kann. Die wählbaren Adressbereiche umfassen Segmente der nicht weiterleitbaren IP-Standardadressbereiche.

Neben diesen Standardbereichen ist ein besonderer Bereich für IP-Adressen reserviert. Dieser besondere Bereich kann verwendet werden, um in den Fällen Konflikte zu vermeiden, in denen die an die HMC angeschlossenen offenen Netze einen der nicht weiterleitbaren Adressbereiche verwenden. Auf der Grundlage des ausgewählten Bereichs wird der HMC-Netzschnittstelle im privaten Netz automatisch die erste IP-Adresse dieses Bereichs zugewiesen; den Serviceprozessoren werden anschließend Adressen aus dem Rest des Bereichs zugewiesen.

Der DHCP-Server in der HMC verwendet eine automatische Zuordnung. Das bedeutet, dass jeder eindeutigen Ethernet-Schnittstelle des Serviceprozessors bei jedem Start immer dieselbe IP-Adresse zugeordnet wird. Jede Ethernet-Schnittstelle hat eine eindeutige Kennung, die auf einer integrierten MAC-Adresse (Media Access Control) basiert und die es dem DHCP-Server erlaubt, dieselben IP-Parameter erneut zuzuordnen. Sie können beide HMC-Anschlüsse **eth0** und **eth1** für DHCP-Adressen konfigurieren. Sie können beide HMC-Anschlüsse **eth0** und **eth1** für DHCP-Adressen konfigurieren.

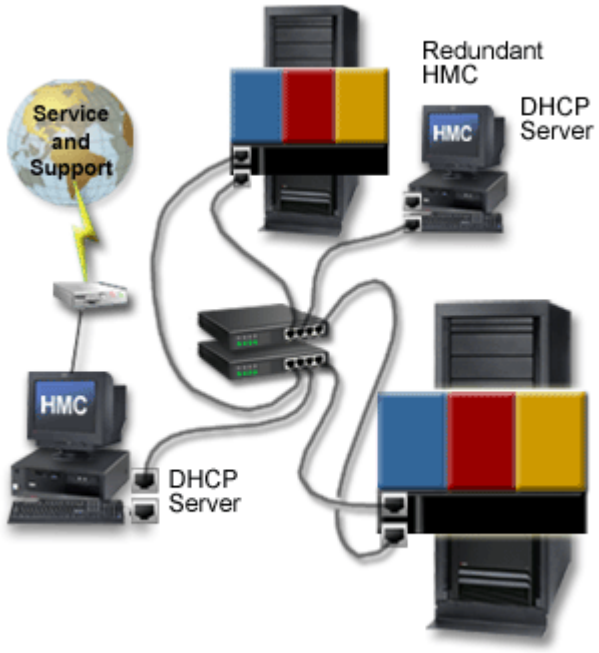
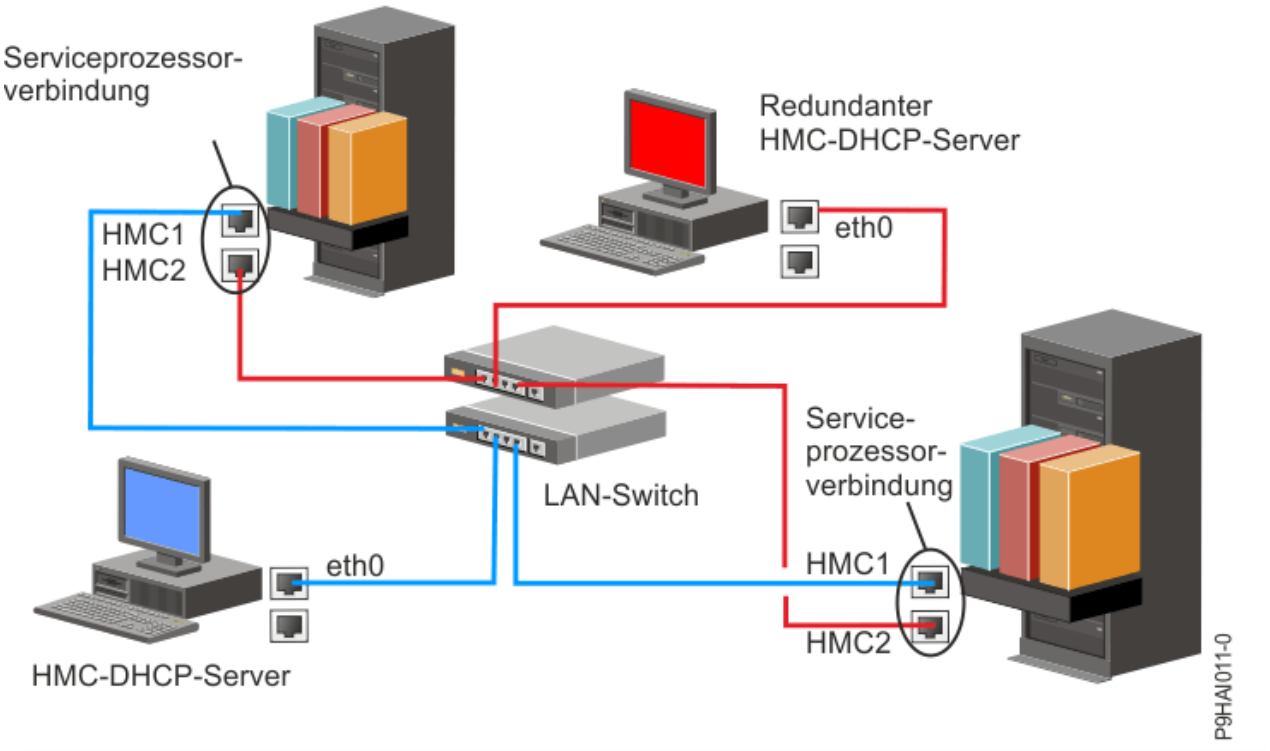


Abbildung 9. Privates Netz mit einer HMC als DHCP-Server

Anmerkung: Wenn Sie IPv6 verwenden, muss der Erkennungsprozess manuell erfolgen. Für IPv6 ist die automatische Erkennung nicht verfügbar.

Weitere Informationen zur Konfiguration der HMC als DHCP-Server finden Sie im Abschnitt „HMC als DHCP-Server konfigurieren” auf Seite 65.



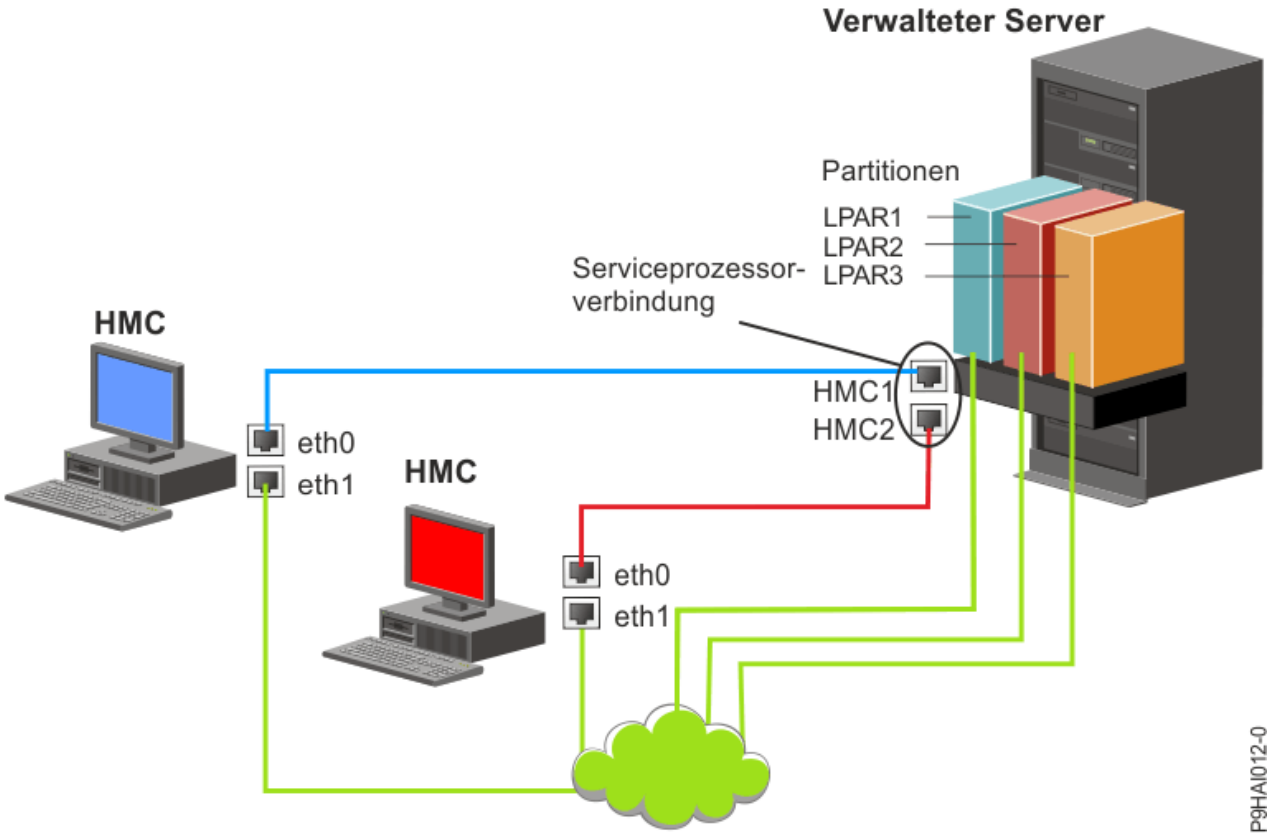
Diese Abbildung zeigt die Umgebung einer redundanten HMC mit zwei verwalteten Systemen. Die erste HMC wird an den ersten Anschluss eines jeden FSPs angeschlossen und die redundante HMC wird an den zweiten Anschluss eines jeden FSPs angeschlossen. Jede HMC ist als DHCP-Server konfiguriert und verwendet IP-Adressen aus einem anderen Bereich. Die Verbindungen befinden sich in separaten privaten

Netzen. Daher muss ungedingt sichergestellt werden, dass bei keinem FSP-Anschluss Verbindungen zu mehreren HMCs vorhanden sind.

Jeder FSP-Anschluss eines verwalteten Systems, an dem eine HMC angeschlossen ist, muss eine eindeutige IP-Adresse aufweisen. Um sicherzustellen, dass jeder FSP eine eindeutige IP-Adresse hat, verwenden Sie die integrierte DHCP-Server-Funktionalität der HMC. Wenn der FSP die aktive Netzverbindung feststellt, gibt er eine Broadcastanforderung aus, um einen DHCP-Server zu suchen. Sofern die HMC ordnungsgemäß konfiguriert ist, reagiert sie auf diese Anforderung, indem sie eine Adresse eines bestimmten Adressenbereichs zuordnet.

Sind mehrere FSPs vorhanden, ist für das private Netz von HMC zu FSP ein eigener LAN-Switch oder Hub erforderlich. Alternativ kann dieses private Segment als verschiedene Anschlüsse in einem privaten *virtuellen LAN* (VLAN) auf einem größeren verwalteten Switch vorhanden sein. Sind mehrere private VLANs vorhanden, müssen Sie sicherstellen, dass sie isoliert sind und kein übergreifender Datenverkehr stattfindet.

Wenn Sie eine Umgebung mit mehreren HMCs haben, müssen Sie auch jede HMC an die logischen Partitionen sowie untereinander in demselben offenen Netz anschließen.



Diese Abbildung zeigt zwei HMCs, die an einen verwalteten Server in dem privaten Netz und an drei logische Partitionen in dem öffentlichen Netz angeschlossen sind. Sie können zusätzliche Ethernet-Adapter für die HMC verwenden, um so drei Netzschnittstellen zu haben. Sie können dieses dritte Netz als ein Verwaltungsnetz verwenden oder es mit dem CSM-Management-Server (CSM = Cluster Systems Manager) verbinden.

Konnektivitätsmethode für den Call-Home-Server auswählen

Hier erfahren Sie mehr über die Konnektivitätsoptionen, die Ihnen bei Verwendung des Call-Home-Servers zur Verfügung stehen.

Sie können die Hardware Management Console (HMC) so konfigurieren, dass auf Hardware-Service bezogene Informationen unter Verwendung einer LAN-basierten Internetverbindung oder einer Wählverbindung über Modem an IBM gesendet werden können.

Bei der Konfiguration der LAN-basierten Internetverbindung haben Sie zwei Auswahlmöglichkeiten hinsichtlich der Datenübertragung. Die erste Auswahlmöglichkeit ist die Verwendung von Standard-SSL (Secure Sockets Layer). Die SSL-Kommunikation kann für die Verbindung zum Internet über Ihren Proxy-Server aktiviert werden. SSL-Konnektivität ist wahrscheinlich eher mit den unternehmensinternen Sicherheitsrichtlinien konform.

Anmerkung: Wenn Ihre offene Netzschnittstellenverbindung nur IPv6 (Internet Protocol Version 6) verwendet, können Sie für die Verbindung zum Support kein Internet-VPN verwenden. Weitere Informationen zu den verwendeten Protokollen finden Sie im Abschnitt „Internetprotokoll auswählen” auf Seite 46.

Die Verwendung einer Internetverbindung kann folgende Vorteile bieten:

- Schnellere Übertragungsgeschwindigkeit
- Verringerter Kostenaufwand bei Kunden (zum Beispiel die Kosten einer dedizierten analogen Telefonleitung)
- Größere Zuverlässigkeit

Unabhängig von der gewählten Konnektivitätsmethode sind die folgenden Sicherheitsmerkmale gültig:

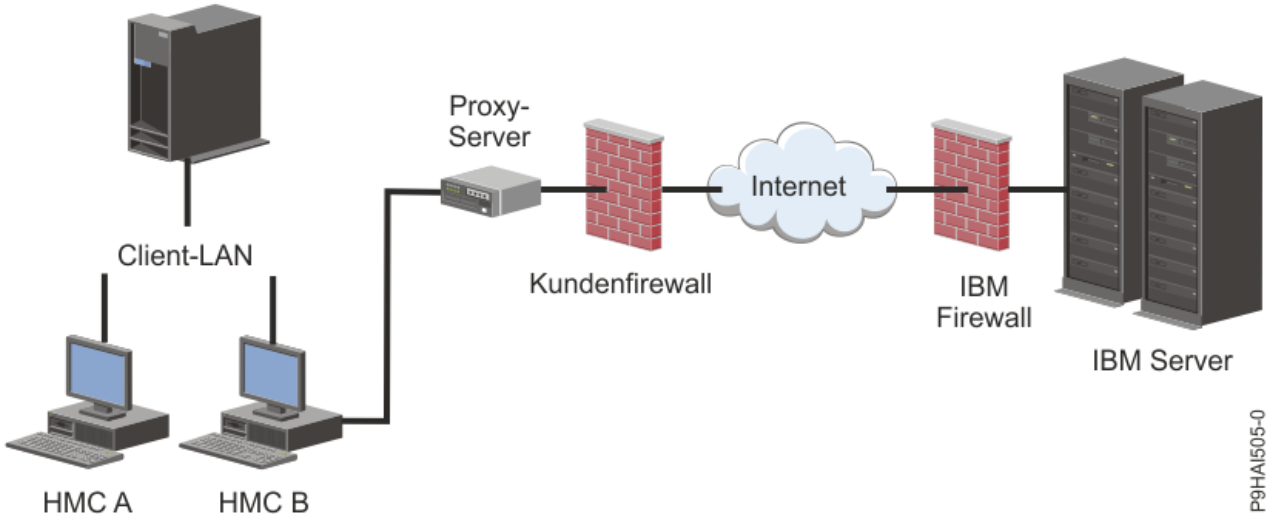
- Remote Support Facility-Anforderungen an IBM werden immer von der HMC eingeleitet. Eine eingehende Verbindung wird nie von dem IBM Serviceunterstützungssystem eingeleitet.
- Für alle Daten, die zwischen der HMC und dem IBM Serviceunterstützungssystem übertragen werden, wird eine hochwertige Verschlüsselungsmethode verwendet. Abhängig von der ausgewählten Konnektivitätsmethode werden die Daten entweder mit SSL oder mit IPSec Encapsulating Security Payload (ESP) verschlüsselt.
- Bei der Einleitung der verschlüsselten Verbindung authentifiziert die HMC als Ziel das IBM Service Support System.

Bei den an das IBM Serviceunterstützungssystem gesendeten Daten handelt es sich ausschließlich um Daten zu Hardwarefehlern und Konfiguration. Es werden keine Anwendungs- oder Kundendaten an IBM übertragen.

Indirekte Internetverbindung mit Proxy-Server verwenden

Wenn bei Ihrer Installation die HMC in einem privaten Netz sein muss, können Sie vielleicht indirekt eine Verbindung zum Internet herstellen, indem Sie einen SSL-Proxy verwenden, der Anforderungen an das Internet weiterleiten kann. Einer der weiteren potentiellen Vorteile bei der Verwendung eines SSL-Proxy liegt darin, dass der Proxy-Server Protokollierungs- und Prüffunktionen unterstützen kann.

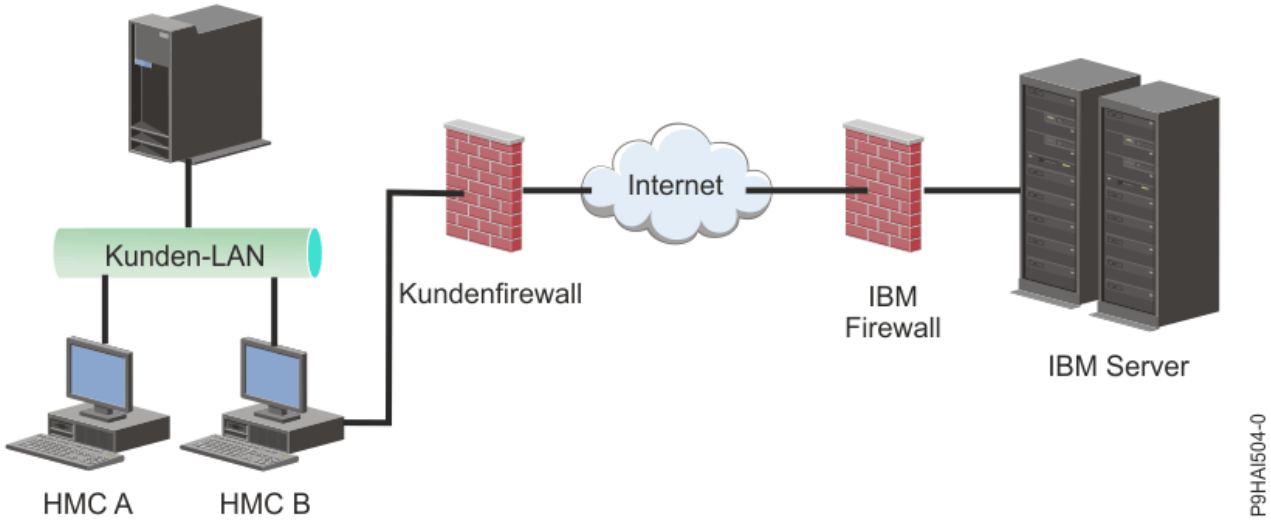
Um SSL-Sockets weiterleiten zu können, muss der Proxy-Server die grundlegenden Proxy-Header-Funktionen (wie in RFC 2616 beschrieben) und die CONNECT-Methode unterstützen. Wahlweise kann die Standard-Proxy-Authentifizierung (RFC 2617) konfiguriert werden, damit die HMC eine Authentifizierung durchführt, bevor Sockets über den Proxy-Server weitergeleitet werden.



Damit die HMC erfolgreich Daten übertragen kann, muss der Proxy-Server des Clients Verbindungen zu Port 443 zulassen. Sie können bei der Konfiguration Ihres Proxy-Servers die speziellen IP-Adressen begrenzen, zu denen die HMC eine Verbindung herstellen kann. Im Abschnitt „Internet-SSL-Adresslisten" auf Seite 46 finden Sie eine Liste von IP-Adressen.

Direkte Internet-SSL-Verbindung verwenden

Sie können eine direkte Internetverbindung verwenden, wenn Ihre HMC eine Verbindung zum Internet herstellen kann und die externe Firewall so eingerichtet werden kann, dass erstellte TCP-Pakete an Zieladressen abgehen können, die unter „Internet-SSL-Adresslisten" auf Seite 46 beschrieben sind.



Mit Internet-SSL eine Verbindung zur fernen Unterstützung herstellen

Alle Datenübertragungen werden über TCP-Sockets vorgenommen, die von der Hardware Management Console (HMC) eingeleitet werden, und für die Verschüsselung der zu übertragenden Daten wird ein hochwertiges SSL verwendet. Die TCP/IP-Zieladressen werden veröffentlicht (siehe „Internet-SSL-Adresslisten" auf Seite 46), damit externe Firewalls für diese Verbindungen konfiguriert werden können.

Anmerkung: Für alle Datenübertragungen wird der HTTPS-Standardanschluss 443 verwendet.

Die HMC kann für eine direkte Verbindung zum Internet oder für eine indirekte Verbindung über einen vom Kunden bereitgestellen Proxy-Server aktiviert werden. Die Entscheidung, welcher Ansatz der beste für Ihre Installation ist, hängt von den unternehmensinternen Anforderungen an Sicherheit und Netzbetrieb ab. Die HMC verwendet (direkt oder über den SSL-Proxy) die folgenden Adressen, wenn sie für die Verwendung von Internet-SSL-Konnektivität konfiguriert wurde.

Internetprotokoll auswählen

Geben Sie die IP-Adresse an, die für die Herstellung der Verbindung zwischen der Hardware Management Console (HMC) und Ihrem Service-Provider verwendet wird.

Die meisten Benutzer verwenden IPv4 (Internet Protocol Version 4) für die Herstellung der Verbindung zu einem Service-Provider. IPv4-Adressen erscheinen für den Zugriff auf das Internet in dem Format, das die 4 Bytes der IPv4-Adresse, durch Punkte getrennt (zum Beispiel 9.60.12.123), darstellt. Sie können auch IPv6 (Internet Protocol Version 6) für die Herstellung der Verbindung zum Service-Provider verwenden. IPv6 wird oft von Netzadministratoren verwendet, um einen eindeutigen Adressraum sicherzustellen. Wenden Sie sich an Ihren Netzadministrator, wenn Sie nicht sicher sind, welches Internetprotokoll bei der Installation verwendet wird. Weitere Informationen über die Verwendung der einzelnen Versionen finden Sie in den Abschnitten „IPv4-Adresse festlegen" auf Seite 66 und „IPv6-Adresse festlegen" auf Seite 66.

Internet-SSL-Adresslisten

Dieser Abschnitt enthält Informationen zu den Adressen, die von der Hardware Management Console (HMC) verwendet werden, wenn die HMC die Internet-SSL-Konnektivität verwendet.

Wenn die HMC für die Verwendung von Internet-SSL-Konnektivität konfiguriert wurde, verwendet sie die folgenden IPv4-Adressen für die Kontaktaufnahme mit IBM Service und Support:

Die folgenden IPv4-Adressen gelten für alle Standorte:

- 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

Die folgenden IPv4-Adressen gelten für Nord- und Südamerika:

- 129.42.160.48
- 129.42.160.49
- 207.25.252.197
- 207.25.252.200
- 207.25.252.204

Die folgenden IPv4-Adressen gelten für alle Standorte außer Nord- und Südamerika:

- 129.42.160.48
- 129.42.160.50
- 207.25.252.197
- 207.25.252.200
- 207.25.252.205

Anmerkung: Wenn Sie eine Firewall konfigurieren, um die Verbindung einer HMC mit diesen Servern zu ermöglichen, sind nur die für die geografische Region zutreffenden IP-Adressen erforderlich.

Wenn die HMC für die Verwendung von Internet-SSL-Konnektivität konfiguriert wurde, verwendet sie die folgenden IPv6-Adressen für die Kontaktaufnahme mit IBM Service und Support:

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

Mehrere Call-Home-Server verwenden

In diesem Abschnitt wird beschrieben, was Sie bei der Entscheidung, mehrere Call-Home-Server zu verwenden, wissen müssen.

Zur Vermeidung eines Single Point of Failure konfigurieren Sie die Hardware Management Console (HMC) für die Verwendung mehrerer Call-Home-Server. Der erste verfügbare Call-Home-Server versucht, jedes Service-Ereignis zu verarbeiten. Wenn die Verbindung oder Übertragung bei diesem Call-Home-Server fehlschlägt, wird die Serviceanforderung mit den anderen verfügbaren Call-Home-Servern erneut versucht, bis die Anforderung erfolgreich durchgeführt werden kann oder bis alle Server ausprobiert wurden.

Die angeschlossene HMC, die bei der Fehleranalyse als primäre analysierende Konsole für ein bestimmtes verwaltetes System ausgewiesen wurde, das den Fehler meldet. Diese primäre Konsole repliziert auch den Fehlerbericht für eine sekundäre HMC. Diese sekundäre HMC muss im Netz von der primären Konsole erkannt werden. Eine sekundäre HMC wird von der primären HMC als ein zusätzlicher Call-Home-Server erkannt, wenn Folgendes der Fall ist:

- Die primäre HMC wurde für die Verwendung von "entdeckten" Call-Home-Servern konfiguriert und der Call-Home-Server befindet sich entweder in demselben Teilnetz wie die primäre HMC oder verwaltet dasselbe System.

- Der Call-Home-Server wurde in der Liste mit Call-Home-Serverkonsolen, die für Konnektivität nach außen verfügbar sind, manuell hinzugefügt.

HMC-Konfiguration vorbereiten

Hier erhalten Sie Informationen zu den erforderlichen Konfigurationseinstellungen, die Sie vor Beginn der Konfiguration kennen müssen.

Um die HMC konfigurieren zu können, müssen Sie mit den zugehörigen Konzepten vertraut sein, Entscheidungen treffen und Informationen vorbereiten.

Hier erhalten Sie die Informationen, die für den Anschluss der HMC an folgende Einrichtungen erforderlich sind:

- Serviceprozessoren in verwalteten Systemen
- Logische Partitionen auf diesen verwalteten Systemen
- Ferne Workstations
- IBM Service zur Implementierung von Call-Home-Funktionen

Führen Sie die folgenden Schritte aus, um die HMC-Konfiguration vorzubereiten:

1. Besorgen und installieren Sie den neuesten Stand der HMC-Code-Version, den Sie installieren möchten.
2. Bestimmen Sie den physischen Standort der HMC in Bezug auf die zu verwaltenden Server. Wenn die HMC mehr als 7,5 Meter von dem verwalteten System entfernt ist, müssen Sie für das verwaltete System einen Web-Browser-Zugriff auf die HMC einrichten, damit die Kundendienstmitarbeiter auf die HMC zugreifen können.
3. Bestimmen Sie die Server, die von der HMC verwaltet werden sollen.
4. Bestimmen Sie, ob Sie ein privates oder ein offenes Netz zur Verwaltung der Server verwenden werden. Wenn Sie sich für ein privates Netz entscheiden, nehmen Sie DHCP, sofern Sie nicht eine CSM-Konfiguration (CSM = Cluster System Management) verwenden. IPv6 wird von CSM nicht unterstützt. Sie benötigen zwei Netze, um auf CSM zugreifen zu können. Weitere Informationen über CSM finden Sie in der mit diesem Feature bereitgestellten Dokumentation. Weitere Informationen über private und offene Netze finden Sie unter „Privates oder offenes Netz auswählen” auf Seite 65.
5. Wenn Sie ein offenes Netz zur Verwaltung eines FSPs verwenden, müssen Sie die Adresse des FSPs manuell über die ASMI-Menüs festlegen. Ein privates Netz mit nicht weiterleitbaren IP-Adressen wird empfohlen.
6. Wenn Sie zwei HMCs haben, bestimmen Sie eine primäre und eine sekundäre HMC. Die primäre HMC sollte sich näher am System befinden und es sollte sich um die HMC handeln, die für die Call-Home-Funktion konfiguriert wurde.
7. Legen Sie die Netzeinstellungen fest, die Sie für den Anschluss der HMC an ferne Workstations, logische Partitionen und Netzeinheiten benötigen werden.
8. Legen Sie fest, wie die Call-Home-Funktion für die HMC aussehen soll. Zu den Call-Home-Optionen gehören die SSL-Internetverbindung mit ausschließlich abgehenden Daten, ein Modem oder eine VPN-Verbindung.
9. Bestimmen Sie die HMC-Benutzer, die Sie erstellen werden, sowie ihre Kennwörter und auch die ihnen zugeordneten Berechtigungsklassen. Sie müssen den Benutzern **hscroot** und **hscpe** ein Kennwort zuordnen.
10. Dokumentieren Sie die folgenden Kontaktinformationen des Unternehmens, die für die Konfiguration der Call-Home-Funktion erforderlich sind:
    - Firmenname
    - Administrator (Kontaktinformation)
    - E-Mail-Adresse
    - Telefonnummern

- Faxnummern
- Straße und Hausnummer des physischen Standorts der HMC

11. Wenn Sie vorhaben, Bediener oder Systemadministratoren per E-Mail zu benachrichtigen, wenn Informationen über die Call-Home-Funktion an IBM Service gesendet werden, geben Sie den SMTP-Server und die E-Mail-Adressen an, die Sie verwenden werden.
12. Sie müssen die folgenden Kennwörter festlegen:
    - Das Zugriffskennwort, das zur Authentifizierung der HMC beim FSP verwendet wird.
    - Das ASMI-Kennwort, das für den Benutzer mit Administratorberechtigung (**admin**) verwendet wird.
    - Das ASMI-Kennwort, das für den Endbenutzer (**general**) verwendet wird.

    Erstellen Sie die Kennwörter, wenn Sie zum ersten Mal eine Verbindung von der HMC zu einem neuen Server herstellen. Handelt es sich bei der HMC um eine redundante oder zweite HMC, besorgen Sie sich das HMC-Benutzerkennwort und halten Sie es zur Eingabe bereit, wenn Sie zum ersten Mal eine Verbindung zum FSP des verwalteten Servers herstellen.

Fahren Sie mit „Arbeitsblatt zur Konfiguration bei der Installationsvorbereitung für die HMC” auf Seite 49 fort, wenn Sie mit diesen Vorbereitungen fertig sind.

Arbeitsblatt zur Konfiguration bei der Installationsvorbereitung für die HMC

Mit diesem Arbeitsblatt können Sie die benötigten Informationen für die Installation bereithalten.

Verbesserte Kennwortrichtlinie für die HMC

Sie müssen bei der ersten Nutzung eines neu hergestellten Systems mit einer HMC ab Version 9.940.0 und nach der Zurücksetzung des Systems auf die Werkseinstellungen ein neues Kennwort festlegen. Mithilfe dieser Richtlinienänderung soll durchgesetzt werden, dass die HMC nicht in einem Status mit einem bekannten Kennwort verbleibt.

Bei HMC ab Version 9.940.0 ist das Kennwort `hscroot` abgelaufen. Das Kennwort muss geändert werden, bevor Sie auf die Funktionen der HMC zugreifen können. Weitere Informationen zum Ändern des Kennworts finden Sie unter https://www.ibm.com/support/knowledgecenter/POWER9/p9eh6/p9eh6_useridsandpassword.htm. Wenn Sie jedoch ein Upgrade von einer Vorgängerversion der HMC oder einer betriebsbereiten Installation durchführen, müssen Sie das Kennwort nicht ändern.

Netzeinstellungen

LAN-Schnittstelle: Wählen Sie die verfügbaren Adapter (wie z. B. eth0, eth1) aus, die von dieser HMC verwendet werden, um eine Verbindung zu verwalteten Systemen, logischen Partitionen, Service und Support und fernen Benutzern herzustellen. Weitere Informationen finden Sie unter „HMC-Netzverbindungen” auf Seite 39. Konnektivität kann bei der HMC entweder in einem privaten oder in einem öffentlichen Netz gegeben sein.

Übertragungsgeschwindigkeit und Duplexmodus für Ethernet-Adapter
Geben Sie die gewünschte Übertragungsgeschwindigkeit und den gewünschten Duplexmodus für Ethernet-Adapter ein. Die Option "Automatische Erkennung" bestimmt, welche Auswahl optimal ist, wenn Sie sich nicht sicher sind, welche Übertragungsgeschwindigkeit und welcher Duplexmodus für Ihre Hardware die besten Ergebnisse bringt. Standardwert = Automatische Erkennung. "Leitungsgeschwindigkeit" gibt die Übertragungsgeschwindigkeit eines Ethernet-Adapters im Duplexmodus an. Wenn Sie keine feste Leitungsgeschwindigkeit angeben müssen, wählen Sie "Automatische Erkennung" aus. Der Modus aller an den FSP angeschlossenen Einheiten (Switches/HMC) muss auf "Automatisch (Geschwindigkeit)/Automatisch (Duplex)" festgelegt werden. Dies ist die FSP-Standardeinstellung und kann nicht geändert werden.

Tabelle 10. Übertragungsgeschwindigkeit und Duplexmodus für Ethernet-Adapter

Merkmal	**eth0**	**eth1**	**eth2**	**eth3**
Übertragungsgeschwindigkeit und Duplexmodus auswählen				

Tabelle 10. Übertragungsgeschwindigkeit und Duplexmodus für Ethernet-Adapter (Forts.)				
Merkmal	**eth0**	**eth1**	**eth2**	**eth3**
Leitungsgeschwindigkeit (Automatische Erkennung, 10/100/1000 Voll-/Halbduplex)				

Weitere Informationen über private und offene Netze finden Sie unter „Private und offene Netze in der HMC-Umgebung” auf Seite 41.

Tabelle 11. Privates oder offenes Netz				
Merkmal	**eth0**	**eth1**	**eth2**	**eth3**
Geben Sie für jeden Adapter ein **Privat**es oder **Öffentlich**es bzw. offenes Netz an.				

DHCP (Dynamic Host Configuration Protocol) stellt eine automatisierte Methode für die dynamische Clientkonfiguration zur Verfügung. Sie können diese HMC als DHCP-Server angeben. Wenn es sich um die erste oder die einzige HMC in dem privaten Netz handelt, müssen Sie die HMC als DHCP-Server aktivieren. Wenn Sie die HMC als DHCP-Server aktivieren, werden die verwalteten Systeme in diesem Netz von der HMC automatisch konfiguriert und erkannt.

Für Ethernet-Adapter, die als privates Netz angegeben sind, füllen Sie die folgende Tabelle aus:

Tabelle 12. DHCP-Server		
Kenndaten	**eth0**	**eth1**
Möchten Sie diese HMC als DHCP-Server angeben? (ja/nein)		
Wenn "Ja", notieren Sie den Bereich der IP-Adressen, die verwendet werden sollen.		

Wenn Sie die HMC 7063-CR1 verwenden, müssen Sie den Ethernet-Port **IPMI** mit einem Netz verbinden, um auf den Baseboard-Management-Controller (BMC) auf der HMC Zugriff zu haben. Weitere Informationen finden Sie unter „BMC-Konnektivität konfigurieren” auf Seite 66. Füllen Sie die folgende Tabelle für Ihre BMC-Verbindung aus.

Tabelle 13. BMC-Verbindung	
Kenndaten	**IPMI**
Möchten Sie diese Verbindung über den DHCP-Modus konfigurieren? (ja/nein)	
Bei "nein" listen Sie die nachfolgend angegebenen statischen Adressen auf:	
IP-Adresse:	
Teilnetzmaske:	
Gateway:	

Für Ethernet-Adapter, die als *öffentliche* Netze angegeben sind, füllen Sie die folgenden Tabellen aus. Weitere Informationen zu den verschiedenen Versionen der Internetprotokolle finden Sie im Abschnitt „HMC-Netztypen konfigurieren” auf Seite 60.

Verwendung von IPv6

Wenn Sie IPv6 verwenden, sprechen Sie mit Ihrem Netzadministrator und entscheiden Sie dann, wie Sie IP-Adressen erhalten wollen. Füllen Sie anschließend die folgenden Tabellen aus:

Tabelle 14. IPv6 (statisch)

Merkmal	**eth0**	**eth1**	**eth2**	**eth3**
Verwenden Sie eine statisch zugeordnete IP-Adresse? Wenn ja, tragen Sie diese Adresse hier ein.				

Tabelle 15. IPv6 (DHCP-Server)

Merkmal	**eth0**	**eth1**	**eth2**	**eth3**
Erhalten Sie IP-Adressen von einem DHCP-Server? (Ja/Nein)				

Tabelle 16. IPv6 (IPv6-Router)

Merkmal	**eth0**	**eth1**	**eth2**	**eth3**
Erhalten Sie IP-Adressen von einem IPv6-Router?				

Weitere Informationen über das Festlegen von IPv6-Adressen finden Sie unter „IPv6-Adresse festlegen” auf Seite 66. Weitere Informationen über die ausschließliche Verwendung von IPv6-Adressen erhalten Sie unter „Ausschließliche Verwendung von IPv6-Adressen” auf Seite 67.

Verwendung von IPv4

Für Ethernet-Adapter, die als öffentliche Netze mit Verwendung von IPv4 angegeben sind, füllen Sie die folgenden Tabellen aus.

Tabelle 17. IPv4

Kenndaten	**eth0**	**eth1**	**eth2**	**eth3**
Möchten Sie eine IP-Adresse automatisch abrufen? (ja/nein)				
Bei "nein" listen Sie die nachfolgend angegebenen Adressen auf:				
TCP/IP-Schnittstellenadresse:				
TCP/IP-Schnittstelle, Netzmaske:				
Firewall-Einstellungen:				

Tabelle 17. IPv4 (Forts.)				
Kenndaten	**eth0**	**eth1**	**eth2**	**eth3**
Möchten Sie die HMC-Firewall-Einstellungen konfigurieren? (ja/nein)				
Bei "Ja" listen Sie die Anwendungen und IP-Adressen auf, die von der Firewall zugelassen werden sollen:				

TCP/IP-Informationen
Für jeden Knoten ist eine eindeutige TCP/IP-Adresse erforderlich, sowohl für Support Element (SE) als auch für Hardware Management Console (HMC). Anhand der zugeordneten Netzmaske wird eine eindeutige Adresse standardmäßig für das lokale private LAN generiert. Wenn die Knoten in ein größeres Netz mit einer verwalteten TCP/IP-Adresse eingebunden werden, können Sie die zu verwendende TCP/IP-Adresse angeben. Der Standardwert wird vom System generiert.

Firewall-Einstellungen
HMC-Firewall-Einstellungen errichten eine Sicherheitsbarriere, die den Zugriff auf bestimmte Netzanwendungen auf der HMC erlaubt oder verweigert. Sie können diese Kontrolleinstellungen individuell für jede physische Netzschnittstelle angeben. So können Sie kontrollieren, auf welche HMC-Netzanwendungen in den einzelnen Netzen zugegriffen werden kann.

Wenn Sie wenigstens einen Adapter als Adapter für ein öffentliches Netz konfiguriert haben, müssen Sie die folgenden zusätzlichen Informationen bereitstellen, um Ihrer HMC den Zugriff auf das LAN zu ermöglichen:

Tabelle 18. Adapter für ein offenes Netz	
Angaben zum lokalen Host	
HMC-Hostname:	
Domänenname:	
Beschreibung der HMC:	
Angaben zum Gateway	
Gatewayadresse: (nnn.nnn.nnn.nnn)	
Gatewayeinheit:	
DNS-Unterstützung	
Möchten Sie DNS nutzen? (ja/nein)	
Bei "ja" geben Sie unten die Reihenfolge für die Suche nach dem DNS-Server an:	
1.	
2.	
Domänensuffix-Suchreihenfolge:	
1.	
2.	

Angaben zum lokalen Host
Um Ihre Hardware Management Console (HMC) für das Netz zu identifizieren, geben Sie den Host- und den Domänennamen der HMC ein. Sofern Sie in Ihrem Netz nicht nur kurze Hostnamen verwenden, geben Sie einen vollständig qualifizierten Hostnamen ein. Beispiel für einen Domänennamen: name.ihrefirma.com

Angaben zum Gateway
Um ein Standardgateway zu definieren, geben Sie die TCP/IP-Adresse ein, die zur Weiterleitung von IP-Paketen verwendet werden soll. Die Gatewayadresse informiert jeden Computer oder jede Netzeinheit, wohin die Daten gesendet werden sollen, wenn sich die Zielstation nicht in demselben Teilnetz wie die Quelle befindet.

DNS-Unterstützung
Das Domain Name System (DNS) stellt eine Standard-Namenskonvention für die Suche nach IP-basierten Computern bereit. Durch Definition von DNS-Servern können Sie Hostnamen anstelle von IP-Adressen zur Bestimmung von Servern und HMCs verwenden.

DNS-Server-Suchreihenfolge
Geben Sie die IP-Adressen von DNS-Servern ein, die für die Zuordnung der Hostnamen und IP-Adressen durchsucht werden sollen. Diese Suchreihenfolge ist nur bei aktiviertem DNS verfügbar.

Reihenfolge für Suche nach Domänensuffixen:
Geben Sie die Domänensuffixe ein, die Sie verwenden. Die HMC verwendet Domänensuffixe, die bei DNS-Suchen an nicht qualifizierte Namen anhängt werden. Die Suffixe werden in der Reihenfolge gesucht, in der sie aufgelistet sind. Diese Suchreihenfolge ist nur bei aktiviertem DNS verfügbar.

E-Mail-Benachrichtigung

Geben Sie E-Mail-Kontaktinformationen ein, wenn Sie per E-Mail über Hardwarefehler auf Ihrem System benachrichtigt werden möchten.

Tabelle 19. E-Mail-Benachrichtigung

Kenndaten	**Eingabefeld**
E-Mail-Adressen:	
SMTP-Server:	
Anschluss:	
Zu berichtende Fehler:	
Nur Fehlerereignisse für Call-Home-Funktion	
Alle Fehlerereignisse	

SMTP-Server
Geben Sie die SMTP-Adresse (Simple Mail Transfer Protocol) des Servers ein, um über ein Systemereignis informiert zu werden. Ein Beispiel für einen SMTP-Servernamen ist `relay.us.ibm.com`.

SMTP ist das Protokoll, das zum Versenden von E-Mails verwendet wird. Wenn Sie SMTP verwenden, versendet ein Client eine Nachricht und kommuniziert dabei über das SMTP-Protokoll mit dem SMTP-Server.

Wenden Sie sich an Ihren Netzadministrator, wenn Sie die SMTP-Adresse Ihres Servers nicht kennen oder wenn Sie nicht sicher sind, wie die SMTP-Adresse Ihres Servers lautet.

Anschluss
Geben Sie die Anschlussnummer des Servers ein, der bei einem Systemereignis benachrichtigt werden soll, oder verwenden Sie den Standardanschluss.

Zu benachrichtigende E-Mail-Adressen
Geben Sie konfigurierten E-Mail-Adressen ein, die bei einem Systemereignis benachrichtigt werden sollen.

- Wählen Sie **Nur Fehlerereignisse für Call-Home-Funktion** aus, um Benachrichtigungen nur dann zu erhalten, wenn Ereignisse in Zusammenhang mit der Call-Home-Funktion auftreten.
- Wählen Sie **Alle Fehlerereignisse** aus, um Benachrichtigungen bei jedem Ereignis zu erhalten.

Servicekontaktinformationen

Tabelle 20. Servicekontaktinformationen

Kenndaten	**Eingabefeld**
Firmenname	
Name des Administrators	
E-Mail-Adresse	
Telefonnummer	
Alternative Telefonnummer	
Faxnummer	
Alternative Telefonnummer	
Straße und Hausnummer	
Straße und Hausnummer 2	
Ort	
Bundesland	
Postleitzahl	
Land	
Standort der HMC (wenn dieser mit der oben angegebenen Adresse des Administrators identisch ist, "gleich" angeben):	
Straße und Hausnummer	
Straße und Hausnummer 2	
Ort	
Bundesland	
Postleitzahl	
Land	

Serviceautorisierung und Konnektivität

Wählen Sie den Verbindungstyp aus, über den der Kontakt mit dem Service-Provider hergestellt werden soll. Eine Beschreibung dieser Methoden einschließlich der Sicherheitsmerkmale und Konfigurationsanforderungen finden Sie im Abschnitt „Vorhandene Call-Home-Server für die Verbindung zu Service und Support für diese HMC auswählen” auf Seite 73.

Tabelle 21. Serviceautorisierung und Konnektivität

Kenndaten	**Eingabefeld**
SSL (Secure Sockets Layer) über das Internet	_____

Tabelle 21. Serviceautorisierung und Konnektivität (Forts.)	
Kenndaten	**Eingabefeld**
VPN (virtuelles privates Netz) über das Internet	_____

SSL (Secure Sockets Layer) über das Internet:
Wenn Sie von Ihrer HMC aus eine Verbindung zum Internet haben, können Sie diese für den Anruf bei Ihrem Service-Provider verwenden. Sie können über verschlüsseltes SSL (Secure Sockets Layer) eine direkte Verbindung zu Ihrem Service-Provider herstellen, indem Sie die vorhandene Internetverbindung verwenden. Wählen Sie **SSL-Proxy verwenden** aus, wenn Sie die Verwendung von SSL-Verschlüsselung über eine indirekte Verbindung mit einem SSL-Proxy konfigurieren möchten.

Tabelle 22. SSL	
Kenndaten	**Eingabefeld**
SSL-Proxy verwenden? (ja/nein)	
Bei "ja" listen Sie die nachfolgend angegebenen Informationen auf:	
Adresse:	
Anschluss:	
Mit SSL-Proxy authentifizieren?	
Bei "ja" listen Sie die nachfolgend angegebenen Informationen auf:	
Benutzer:	
Kennwort:	

Verwendetes Internetanschlussprotokoll

Weitere Informationen zu den verschiedenen Internetprotokollen finden Sie unter „HMC-Netztypen konfigurieren” auf Seite 60.

___ IPv4

___ IPv6

___ IPv4 und IPv6

Virtual Private Network (VPN)
Wenn Sie von Ihrer HMC aus eine Verbindung zum Internet haben, können Sie diese für den Anruf bei Ihrem Service-Provider verwenden. Sie können über VPN (Virtual Private Network) eine direkte Verbindung zu Ihrem Service-Provider herstellen, indem Sie die vorhandene Internetverbindung verwenden.

Anmerkung: Wenn Sie VPN (Virtual Private Network) über das Internet auswählen, können Sie keine weitere Option auswählen.

Call-Home-Server

Legen Sie fest, welche HMCs Sie für die Verbindung zu Service und Support als Call-Home-Server konfigurieren möchten. Weitere Informationen über die Verwendung von mehreren Call-Home-Servern finden Sie unter „Mehrere Call-Home-Server verwenden” auf Seite 47.

___ Diese HMC

___ Weitere HMC

Wenn Sie **Weitere HMC** markiert haben, listen Sie hier die anderen HMCs auf, die als Call-Home-Server konfiguriert wurden:

Tabelle 23. Weitere als Call-Home-Server konfigurierte HMCs
Liste der Hostnamen oder IP-Adressen von HMCs, die als Call-Home-Server konfiguriert wurden

Zusätzliche Unterstützungsleistungen

My Systems und Premium Search

Tabelle 24. My Systems und Premium Search	
Kenndaten	**Eingabefeld**
Geben Sie Ihre IBM ID an	_____
Geben Sie weitere IBM IDs an	_____

Um auf wertvolle, angepasste Unterstützungsinformationen in den Abschnitten "My Systems" und "Premium Search" der Website von Electronic Services zugreifen zu können, müssen Kunden ihre IBM ID bei diesem System registrieren. Falls Sie noch keine IBM ID besitzen, können Sie sich für eine IBM ID unter www.ibm.com/account/profile registrieren.

Anmerkung: IBM stellt angepasste Webfunktionen bereit, die von der Anwendung IBM Electronic Service Agent gesammelte Informationen verwenden. Damit Sie diese Funktionen verwenden können, müssen Sie sich zunächst auf der IBM Registrierungswebsite unter http://www.ibm.com/account/profile registrieren.

Um Benutzer für die Verwendung der Informationen des Electronic Service Agent für die Anpassung der Webfunktionen zu autorisieren, geben Sie Ihre IBM ID ein, die Sie auf der IBM Registrierungswebsite registriert haben. Rufen Sie die Website http://www.ibm.com/support/electronic auf, um wertvolle Unterstützungsinformationen abzurufen, die für Kunden, die eine IBM ID für ihre Systeme registrieren, verfügbar sind.

HMC konfigurieren

Hier wird beschrieben, wie Sie Netzverbindungen, Sicherheit, Serviceanwendungen und einige Benutzereinstellungen konfigurieren.

Je nach der Anpassungsstufe der HMC-Konfiguration gibt es mehrere Möglichkeiten, die HMC an Ihre Anforderungen anzupassen. Der Guided Setup Wizard ist ein Tool auf der HMC, das die Konfiguration der HMC erleichtert. Sie können den Direktaufruf durch den Assistenten wählen, um die empfohlene HMC-Umgebung schnell zu erstellen, oder Sie können sich mit den verfügbaren Einstellungen, durch die Sie der Assistent führt, umfassend vertraut machen. Sie können die Konfiguration auch ohne den Assistenten durchführen, indem Sie die HMC mithilfe der HMC-Menüs konfigurieren (siehe HMC mithilfe der HMC-Menüs konfigurieren).

Bevor Sie beginnen, stellen Sie die erforderlichen Konfigurationsdaten zusammen, die Sie zum erfolgreichen Ausführen der Schritte benötigen. Eine Liste der erforderlichen Informationen finden Sie unter „HMC-Konfiguration vorbereiten” auf Seite 48. Wenn Sie mit der Vorbereitung fertig sind, müssen Sie zunächst das „Arbeitsblatt zur Konfiguration bei der Installationsvorbereitung für die HMC” auf Seite 49 durcharbeiten und dann zu diesem Abschnitt zurückkehren.

HMC mithilfe des Direktaufrufs durch den Guided Setup Wizard konfigurieren

In den meisten Fällen kann die HMC so konfiguriert werden, dass sie mit vielen der Standardeinstellungen effizient arbeiten kann. Verwenden Sie diese Prüfliste für Direktaufruf, um die HMC für den Betrieb vorzubereiten. Wenn Sie diese Schritte ausgeführt haben, ist die HMC als DHCP-Server in einem privaten (direkt angeschlossenen) Netz konfiguriert.

HMC mithilfe der Menüs konfigurieren

Dieser Abschnitt enthält eine vollständige Liste aller HMC-Konfigurationstasks, die Sie durch die Konfiguration der HMC führt. Wählen Sie diese Option, wenn Sie den Guided Setup Wizard (Assistent zur Installationsanleitung) nicht verwenden möchten.

Sie müssen die HMC erneut starten, damit die Konfigurationseinstellungen in Kraft treten. Daher ist es sinnvoll, diese Prüfliste zu drucken, um sie bei der Konfiguration der HMC zur Hand zu haben.

Diese Informationen verweisen auf Tasks, die nicht in diesem Dokument enthalten sind. Sie können über die HMC oder das Web auf das IBM Power Systems Hardware Information zugreifen. Auf der HMC kann rechts oben in der Taskleiste auf das IBM Knowledge Center zugegriffen werden. Im Web kann unter https://www.ibm.com/support/knowledgecenter auf das IBM Knowledge Center zugegriffen werden.

Diese Informationen verweisen auf Tasks, die nicht in dieser PDF enthalten sind. Sie können über den Abschnitt **Zusätzliche Ressourcen** auf der HMC-Begrüßungsseite auf weitere Unterstützungsmaterialien zugreifen.

Voraussetzungen

Bevor Sie mit der Konfiguration der HMC mithilfe der HMC-Menüs beginnen, müssen Sie sicherstellen, dass die unter „HMC-Konfiguration vorbereiten” auf Seite 48 beschriebenen Konfigurationsvorbereitungen getroffen wurden.

Tabelle 25. Manuelle HMC-Konfigurationstasks und Referenzinformationen

Task	**Referenzinformationen**
1. Starten Sie die HMC.	„HMC starten” auf Seite 58
2. Legen Sie das Datum und die Uhrzeit fest.	
3. Ändern Sie vordefinierte Kennwörter.	
4. Erstellen Sie weitere Benutzer und kehren Sie zu dieser Prüfliste zurück, wenn Sie diesen Schritt ausgeführt haben.	
5. Konfigurieren Sie Netzverbindungen.	„HMC-Netztypen konfigurieren” auf Seite 60
6. Für HMC-Modell 7063-CR1 müssen Sie die IP-Adresse des Baseboard-Management-Controllers (BMC) konfigurieren.	„BMC-Konnektivität konfigurieren” auf Seite 66
7. Legen Sie die Identifikationsinformationen fest, wenn Sie ein offenes Netz und eine feste IP-Adresse verwenden.	
8. Konfigurieren Sie einen Routing-Eintrag als Standardgateway, wenn Sie ein offenes Netz und eine feste IP-Adresse verwenden.	„Route-Eintrag als Standardgateway konfigurieren” auf Seite 68
9. Konfigurieren Sie Domänennamensservices, wenn Sie ein offenes Netz und eine feste IP-Adresse verwenden.	„Domänennamensservices konfigurieren” auf Seite 69

Tabelle 25. Manuelle HMC-Konfigurationstasks und Referenzinformationen (Forts.)	
Task	**Referenzinformationen**
10. Konfigurieren Sie Domänensuffixe, wenn Sie eine feste IP-Adresse verwenden und DNS aktiviert ist.	„Domänensuffixe konfigurieren” auf Seite 69
11. Konfigurieren Sie Ihren Server für die Verbindung zu Service und Support von IBM und kehren Sie zu dieser Prüfliste zurück, wenn Sie diesen Schritt ausgeführt haben.	„Lokale Konsole für die Fehlermeldung an Service und Support konfigurieren” auf Seite 72
12. Konfigurieren Sie den Ereignismanager für die Call-Home-Funktion.	„Ereignismanager für die Call-Home-Funktion konfigurieren” auf Seite 75
13. Schließen Sie das verwaltete System an einen Versorgungsstromkreis an.	
14. Legen Sie Kennwörter für das verwaltete System sowie die ASMI-Kennwörter (allgemein und Administrator) fest.	„Kennwörter für das verwaltete System festlegen” auf Seite 76
15. Greifen Sie auf die ASMI zu, um Datum und Uhrzeit auf dem verwalteten System einzustellen.	
16. Starten Sie das verwaltete System und kehren Sie zu dieser Prüfliste zurück, wenn Sie diesen Schritt ausgeführt haben.	
17. Stellen Sie sicher, dass eine logische Partition auf dem verwalteten System vorhanden ist.	
18. Optional: Fügen Sie ein weiteres verwaltetes System hinzu und kehren Sie zu dieser Prüfliste zurück, wenn Sie diesen Schritt ausgeführt haben.	
19. Optional: Wenn Sie mit Ihrer HMC einen neuen Server installieren, konfigurieren Sie die logischen Partitionen und installieren Sie das Betriebssystem.	
20. Wenn Sie jetzt keinen neuen Server installieren, führen Sie die optionalen nach der Konfiguration auszuführende Tasks aus, um Ihre Konfiguration weiter anzupassen.	„Nach der Konfiguration auszuführende Schritte” auf Seite 78

HMC starten

Sie können sich an der HMC anmelden und auswählen, welche Sprache für die Schnittstelle verwendet werden soll. Verwenden Sie beim ersten Anmelden an der HMC die Standard-Benutzer-ID `hscroot` und das Standardkennwort `abc123`.

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um die HMC zu starten:

Vorgehensweise

1. Drücken Sie den Netzschalter, um die HMC einzuschalten.
2. Wenn Ihre Sprachvorgabe Englisch ist, fahren Sie mit Schritt 4 fort.

Wenn Sie eine andere Sprache als Englisch verwenden möchten, geben Sie den Wert **2** ein, wenn Sie zur Änderung der Ländereinstellung aufgefordert werden.

Anmerkung: Das Zeitlimit dieser Eingabeaufforderung ist nach 30 Sekunden überschritten, wenn Sie nicht reagieren.

3. Wählen Sie die gewünschte Ländereinstellung aus der Liste im Fenster **Auswahl der Ländereinstellung** aus und klicken Sie auf **OK**. Die Ländereinstellung gibt die Sprache an, die die HMC-Schnittstelle verwendet.
4. Klicken Sie auf **Melden Sie sich bei der Hardware Management Console-Webanwendung an und starten Sie diese**.
5. Melden Sie sich mit der folgenden Standard-Benutzer-ID und dem folgenden Kennwort bei der HMC an:

   ID: `hscroot`
   Kennwort: `abc123`

   HMC Enhanced
   Zeigt die neuere erweiterte grafische Benutzerschnittstelle mit den erweiterten PowerVM-Features an.

   HMC Classic
   Zeigt die grafische Standardbenutzerschnittstelle ohne die erweiterten PowerVM-Features an.

   Anmerkung: Wenn die HMC als DHCP-Server arbeitet, wird beim erstmaligen Herstellen einer Verbindung zum Serviceprozessor das Standardkennwort verwendet.
6. Drücken Sie die Eingabetaste.

Datum und Uhrzeit ändern

Die batteriebetriebene Uhr ist für das Datum und die Uhrzeit der Hardware Management Console (HMC) zuständig. Sie müssen das Datum und die Uhrzeit der Konsole möglicherweise neu einstellen, wenn die Batterie ausgetauscht wurde oder wenn das System physisch in eine andere Zeitzone transportiert wurde. Hier erfahren Sie, wie Sie das Datum und die Uhrzeit der HMC ändern.

Informationen zu diesem Vorgang

Eine Änderung der Datums- und Zeitinformationen hat keine Auswirkungen auf die Systeme und die logischen Partitionen, die von der HMC verwaltet werden.

Führen Sie die folgenden Schritte aus, um das Datum und die Uhrzeit für die HMC zu ändern:

Vorgehensweise

1. Vergewissern Sie sich, dass Sie einer der folgenden Berechtigungsklassen angehören:
   - Superadministrator
   - Ansprechpartner
   - Bediener
   - Betrachter
2. Klicken Sie im Navigationsbereich auf das Symbol **HMC-Verwaltung**  und wählen Sie anschließend **Konsoleneinstellungen** aus.
3. Klicken Sie im Inhaltsteilfenster auf **Datum und Uhrzeit ändern**.
4. Wenn Sie **UTC** im Feld **Uhr** auswählen, wird die Einstellung für die Uhrzeit automatisch auf Sommer-/Winterzeit in der ausgewählten Zeitzone umgestellt. Geben Sie das Datum, die Uhrzeit und die Zeitzone ein und klicken Sie auf **OK**.

Ergebnisse

HMC-Netztypen konfigurieren

Konfigurieren Sie Ihre HMC so, dass sie mit dem verwalteten System, den logischen Partitionen, fernen Benutzern sowie Service und Support kommunizieren kann.

HMC-Einstellungen zur Verwendung eines offenen Netzes für die Verbindung mit dem verwalteten System konfigurieren

Konfigurieren Sie die HMC so, dass sie bei Verwendung eines offenen Netzes eine Verbindung zu einem verwalteten System herstellen und dieses verwalten kann.

Vorbereitende Schritte

Gehen Sie dazu folgendermaßen vor:

Tabelle 26. HMC-Einstellungen zur Verwendung eines offenen Netzes für die Verbindung mit dem verwalteten System konfigurieren

Task	**Referenzinformationen**
1. Entscheiden Sie, welche Schnittstelle Sie für Ihr verwaltetes System verwenden möchten. **eth0** ist die bevorzugte Auswahl.	„Arbeitsblatt zur Konfiguration bei der Installationsvorbereitung für die HMC" auf Seite 49
2. Geben Sie die Ethernet-Anschlüsse für Ihre HMC an.	„Ethernet-Anschluss eth0 identifizieren" auf Seite 63
3. Konfigurieren Sie den Ethernet-Adapter, indem Sie die folgenden Tasks ausführen:	
a. Legen Sie die Leitungsgeschwindigkeit fest.	„Datenübertragungsgeschwindigkeit festlegen" auf Seite 64
b. Wählen Sie den Typ des offenen Netzes aus.	„Privates oder offenes Netz auswählen" auf Seite 65
c. Legen Sie statische Adressen fest.	„IPv6-Adresse festlegen" auf Seite 66
d. Richten Sie die Firewall ein.	„HMC-Firewalleinstellungen ändern" auf Seite 67
e. Konfigurieren Sie den Standardgateway.	„Route-Eintrag als Standardgateway konfigurieren" auf Seite 68
f. Konfigurieren Sie DNS.	„Domänennamensservices konfigurieren" auf Seite 69
4. Konfigurieren Sie weitere Adapter, sofern vorhanden.	
5. Testen Sie die Verbindung zwischen dem verwalteten Server und der HMC.	„Verbindung zwischen HMC und verwaltetem System testen" auf Seite 77

HMC-Einstellungen zur Verwendung eines privaten Netzes für die Verbindung mit dem verwalteten System konfigurieren

Konfigurieren Sie die HMC so, dass sie bei Verwendung eines Privaten Netzes eine Verbindung zu einem verwalteten System herstellen und dieses verwalten kann.

Vorbereitende Schritte

Gehen Sie dazu folgendermaßen vor:

Tabelle 27. HMC-Einstellungen zur Verwendung eines privaten Netzes für die Verbindung mit dem verwalteten System konfigurieren	
Task	**Referenzinformationen**
1. Entscheiden Sie, welche Schnittstelle Sie für Ihr verwaltetes System verwenden möchten.	„Arbeitsblatt zur Konfiguration bei der Installationsvorbereitung für die HMC" auf Seite 49
2. Geben Sie die Ethernet-Anschlüsse für Ihre HMC an.	„Ethernet-Anschluss eth0 identifizieren" auf Seite 63
3. Konfigurieren Sie die HMC als DHCP-Server.	„HMC als DHCP-Server konfigurieren" auf Seite 65
4. Testen Sie die Verbindung zwischen dem verwalteten Server und der HMC.	„Verbindung zwischen HMC und verwaltetem System testen" auf Seite 77

HMC-Einstellungen zur Verwendung eines offenen Netzes für die Verbindung zu logischen Partitionen konfigurieren

Vorbereitende Schritte

Gehen Sie dazu folgendermaßen vor:

Tabelle 28. HMC-Einstellungen zur Verwendung eines offenen Netzes für die Verbindung zu logischen Partitionen konfigurieren	
Task	**Referenzinformationen**
1. Entscheiden Sie, welche Schnittstelle Sie für Ihr verwaltetes System verwenden möchten.	„Arbeitsblatt zur Konfiguration bei der Installationsvorbereitung für die HMC" auf Seite 49
2. Geben Sie die Ethernet-Anschlüsse für Ihre HMC an.	„Ethernet-Anschluss eth0 identifizieren" auf Seite 63
3. Konfigurieren Sie den Ethernet-Adapter, indem Sie die folgenden Tasks ausführen:	
a. Legen Sie die Leitungsgeschwindigkeit fest.	„Datenübertragungsgeschwindigkeit festlegen" auf Seite 64
b. Wählen Sie den Typ des offenen Netzes aus.	„Privates oder offenes Netz auswählen" auf Seite 65
c. Legen Sie statische Adressen fest.	„IPv6-Adresse festlegen" auf Seite 66
d. Richten Sie die Firewall ein.	„HMC-Firewalleinstellungen ändern" auf Seite 67
e. Konfigurieren Sie den Standardgateway.	„Route-Eintrag als Standardgateway konfigurieren" auf Seite 68
f. Konfigurieren Sie DNS.	„Domänennamensservices konfigurieren" auf Seite 69
4. Konfigurieren Sie weitere Adapter, sofern vorhanden.	
5. Testen Sie die Verbindung zwischen dem verwalteten Server und der HMC.	„Verbindung zwischen HMC und verwaltetem System testen" auf Seite 77

HMC-Einstellungen zur Verwendung eines offenen Netzes für die Verbindung zu fernen Benutzern konfigurieren

Vorbereitende Schritte

Gehen Sie dazu folgendermaßen vor:

Tabelle 29. HMC-Einstellungen zur Verwendung eines offenen Netzes für die Verbindung zu fernen Benutzern konfigurieren

Task	**Referenzinformationen**
1. Entscheiden Sie, welche Schnittstelle Sie für Ihr verwaltetes System verwenden möchten.	„Arbeitsblatt zur Konfiguration bei der Installationsvorbereitung für die HMC" auf Seite 49
2. Geben Sie die Ethernet-Anschlüsse für Ihre HMC an.	„Ethernet-Anschluss eth0 identifizieren" auf Seite 63
3. Konfigurieren Sie den Ethernet-Adapter, indem Sie die folgenden Tasks ausführen:	
a. Legen Sie die Leitungsgeschwindigkeit fest.	„Datenübertragungsgeschwindigkeit festlegen" auf Seite 64
b. Wählen Sie den Typ des offenen Netzes aus.	„Privates oder offenes Netz auswählen" auf Seite 65
c. Legen Sie statische Adressen fest.	„IPv6-Adresse festlegen" auf Seite 66
d. Richten Sie die Firewall ein.	„HMC-Firewalleinstellungen ändern" auf Seite 67
e. Konfigurieren Sie den Standardgateway.	„Route-Eintrag als Standardgateway konfigurieren" auf Seite 68
f. Konfigurieren Sie DNS.	„Domänennamensservices konfigurieren" auf Seite 69
g. Konfigurieren Sie Suffixe.	„Domänensuffixe konfigurieren" auf Seite 69
4. Konfigurieren Sie weitere Adapter, sofern vorhanden.	

Call-Home-Servereinstellungen für HMC konfigurieren

Vorbereitende Schritte

Um die Call-Home-Servereinstellungen der HMC so zu konfigurieren, dass eine Fehlermeldung möglich ist, gehen Sie wie folgt vor:

Tabelle 30. Call-Home-Servereinstellungen für HMC konfigurieren

Task	**Referenzinformationen**
1. Vergewissern Sie sich, dass Ihnen alle erforderlichen Kundeninformationen vorliegen.	„Arbeitsblatt zur Konfiguration bei der Installationsvorbereitung für die HMC" auf Seite 49
2. Konfigurieren Sie diese HMC für die Meldung von Fehlern oder wählen Sie einen vorhandenen Call-Home-Server für die Fehlermeldung aus.	„Lokale Konsole für die Fehlermeldung an Service und Support konfigurieren" auf Seite 72 „Vorhandene Call-Home-Server für die Verbindung zu Service und Support für diese HMC auswählen" auf Seite 73
3. Prüfen Sie, ob die Call-Home-Konfiguration funktioniert.	„Prüfen, ob die Verbindung zu Service und Support funktioniert" auf Seite 74

Tabelle 30. Call-Home-Servereinstellungen für HMC konfigurieren (Forts.)	
Task	**Referenzinformationen**
4. Berechtigen Sie Benutzer zum Anzeigen erfasster Systemdaten.	„Benutzer zum Anzeigen erfasster Systemdaten berechtigen” auf Seite 74
5. Planen Sie die Übertragung von Systemdaten.	„Serviceinformationen übertragen” auf Seite 75

Ethernet-Anschluss eth0 identifizieren
Die Ethernet-Verbindung zu dem verwalteten Server muss über den Ethernet-Anschluss hergestellt werden, der auf Ihrer HMC als `eth0` definiert ist.

Wenn Sie keine zusätzlichen Ethernet-Adapter in den PCI-Steckplätzen Ihrer HMC installiert haben, ist der primäre integrierte Ethernet-Anschluss auf der HMC immer als `eth0` oder `eth1` definiert, wenn die HMC als DHCP-Server für Ihre verwalteten Systeme verwendet werden soll.

Wenn weitere Ethernet-Adapter in PCI-Steckplätzen installiert sind, wird der Anschluss abhängig von Position und Typ der installierten Ethernet-Adapter als `eth0` definiert.

Anmerkung: Die folgenden allgemeinen Regeln treffen möglicherweise nicht auf alle Konfigurationen zu.

In der folgenden Tabelle werden die Regeln für Ethernet-Positionen nach HMC-Typ beschrieben.

Tabelle 31. HMC-Typen und zugeordnete Regeln für Ethernet-Position	
HMC-Typ	**Regeln für Ethernet-Position**
In einem Rack installierte HMCs mit zwei integrierten Ethernet-Anschlüssen.	Die HMC unterstützt nur einen zusätzlichen Ethernet-Adapter. • Wenn ein zusätzlicher Ethernet-Adapter installiert wird, wird dieser Anschluss als `eth0` definiert. In diesem Fall wird dann der primäre integrierte Ethernet-Anschluss als `eth1` und der sekundäre integrierte Ethernet-Anschluss als `eth2` definiert. • Wenn der Ethernet-Adapter zwei Anschlüsse aufweist, ist der mit `Act/link A` gekennzeichnete Anschluss als `eth0` definiert. Der mit `Act/link B` gekennzeichnete Anschluss ist `eth1`. In diesem Fall wird dann der primäre integrierte Ethernet-Anschluss als `eth2` und der sekundäre integrierte Ethernet-Anschluss als `eth3` definiert. • Wenn keine Adapter installiert sind, wird der primäre integrierte Ethernet-Anschluss als `eth0` definiert.

Tabelle 31. HMC-Typen und zugeordnete Regeln für Ethernet-Position (Forts.)	
HMC-Typ	**Regeln für Ethernet-Position**
Standalone-Modelle mit einem integrierten Ethernet-Anschluss.	Die Definitionen sind vom Typ des installierten Ethernet-Adapters abhängig: • Wenn nur ein Ethernet-Adapter installiert ist, wird dieser als `eth0` definiert. • Wenn der Ethernet-Adapter zwei Anschlüsse aufweist, ist der mit `Act/link A` gekennzeichnete Anschluss als `eth0` definiert. Der mit `Act/link B` gekennzeichnete Anschluss wäre dann `eth1`. In diesem Fall wird dann der primäre integrierte Ethernet-Anschluss als `eth2` definiert. • Wenn keine Adapter installiert sind, wird der integrierte Ethernet-Anschluss als `eth0` definiert. • Wenn mehrere Ethernet-Adapter installiert wurden, lesen Sie den Abschnitt „Schnittstellenname für einen Ethernet-Adapter festlegen” auf Seite 64.

Schnittstellenname für einen Ethernet-Adapter festlegen
Wenn Sie die HMC als DHCP-Server konfigurieren, kann dieser Server nur über eine Netzschnittstellenkarte (NIC = Network Interface Card) betrieben werden, deren Anschlüsse von der HMC als `eth0` und `eth1` identifiziert werden. Sie müssen eventuell feststellen, an welchen NIC-Anschluss Sie das Ethernet-Kabel anschließen müssen. Im Folgenden erhalten Sie weitere Informationen darüber, wie Sie feststellen können, welche NIC-Anschlüsse von der HMC als `eth0` und `eth1` identifiziert werden.

Informationen zu diesem Vorgang
Führen Sie die folgenden Schritte aus, um festzustellen, welchen Namen die HMC einem Ethernet-Adapter zugeordnet hat:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf das Symbol **HMC-Verwaltung**  und wählen Sie anschließend **Konsoleneinstellungen** aus.
2. Klicken Sie im Inhaltsbereich auf **Netzeinstellungen ändern**.
3. Klicken Sie im Fenster **Netzeinstellungen ändern** auf die Registerkarte **LAN-Adapter**. Der folgende Beispieleintrag zeigt, dass dieser Ethernet-Anschluss als `eth0` identifiziert ist: `Ethernet eth0 52:54:00:fa:b6:8e (<IP-Adresse der HMC>)`.
4. Notieren Sie Ihre Ergebnisse. Wenn Sie die LAN-Adaptereinstellungen anzeigen oder ändern müssen, dann klicken Sie auf **Details**.
5. Klicken Sie auf **OK**.

Datenübertragungsgeschwindigkeit festlegen
In diesem Abschnitt erfahren Sie, wie Sie die Datenübertragungsgeschwindigkeit angeben, die die Geschwindigkeit und den Duplexmodus für den Ethernet-Adapter umfasst.

Vorbereitende Schritte
Der Standardwert für die HMC-Adaptereinstellungen lautet **Automatische Erkennung**. Wenn der betreffende Adapter an einen LAN-Switch angeschlossen wurde, müssen Sie die Switch-Anschlusseinstellungen abgleichen. Führen Sie die folgenden Schritte aus, um die Datenträgergeschwindigkeit und den Duplexmodus festzulegen:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf das Symbol **HMC-Verwaltung**  und wählen Sie anschließend **Konsoleneinstellungen** aus.
2. Klicken Sie im Inhaltsbereich auf **Netzeinstellungen ändern**.
3. Klicken Sie auf die Registerkarte **LAN-Adapter**.
4. Wählen Sie den LAN-Adapter aus, mit dem Sie arbeiten möchten, und klicken Sie auf **Details**.
5. Wählen Sie in der Anzeige mit den Informationen für das lokale Netz (LAN) die **Automatische Erkennung** oder die entsprechende Kombination aus Datenträgergeschwindigkeit und Duplexmodus aus.
6. Klicken Sie auf **OK**.

Privates oder offenes Netz auswählen
Ein *privates Servicenetz* besteht aus der Hardware Management Console (HMC) und den verwalteten Systemen. Ein privates Servicenetz ist auf Konsolen sowie die von ihnen verwalteten Systeme beschränkt und vom Unternehmensnetz getrennt. Ein *offenes Netz* besteht aus Ihrem privaten Servicenetz und Ihrem Unternehmensnetz. Ein offenes Netz kann neben den Konsolen und den verwalteten Systemen weitere Netzendpunkte enthalten und kann sich über mehrere Teilnetze und Netzeinheiten erstrecken.

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um ein privates oder ein öffentliches Netz auszuwählen:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf das Symbol **HMC-Verwaltung**  und wählen Sie anschließend **Konsoleneinstellungen** aus.
2. Klicken Sie im Inhaltsbereich auf **Netzeinstellungen ändern**.
3. Klicken Sie auf die Registerkarte **LAN-Adapter**.
4. Wählen Sie den LAN-Adapter aus, mit dem Sie arbeiten möchten, und klicken Sie auf **Details**.
5. Klicken Sie auf die Registerkarte **LAN-Adapter**.
6. Wählen Sie auf der Seite mit den Informationen für das lokale Netz **Privat** oder **Offen** aus.
7. Klicken Sie auf **OK**.

HMC als DHCP-Server konfigurieren
DHCP (Dynamic Host Configuration Protocol) stellt eine automatisierte Methode für die dynamische Clientkonfiguration zur Verfügung.

Führen Sie die folgenden Schritte aus, um die Hardware Management Console (HMC) als DHCP-Server zu konfigurieren:

1. Klicken Sie im Navigationsbereich auf das Symbol **HMC-Verwaltung**  und wählen Sie anschließend **Konsoleneinstellungen** aus.
2. Klicken Sie im Inhaltsbereich auf **Netzeinstellungen ändern**. Das Fenster "Netzeinstellungen anpassen" wird geöffnet.
3. Wählen Sie den LAN-Adapter aus, mit dem Sie arbeiten möchten, und klicken Sie auf **Details**.
4. Wählen Sie zuerst **Privat** und dann den Netztyp aus.
5. Wählen Sie im Abschnitt "DHCP-Server" die Option **DHCP-Server aktivieren** aus, um die HMC als DHCP-Server zu aktivieren.

Anmerkung: Die HMC kann nur in einem privaten Netz als DHCP-Server konfiguriert werden. Wenn Sie ein offenes Netz verwenden, ist die Option **DHCP-Server aktivieren** nicht verfügbar.

6. Geben Sie den Adressbereich des DHCP-Servers ein.
7. Klicken Sie auf **OK**.

Wenn Sie die HMC auf einem privaten Netz als DHCP-Server konfiguriert haben, müssen Sie prüfen, ob das private HMC-DHCP-Netz richtig konfiguriert ist. Weitere Informationen zum Anschluss der HMC an ein privates Netz finden Sie unter „Privates oder offenes Netz auswählen” auf Seite 65.

Weitere Informationen finden Sie unter „ HMC als DHCP-Server” auf Seite 42.

BMC-Konnektivität konfigurieren
Sie können die Netzeinstellungen auf dem BMC für die Managementkonsole konfigurieren oder anzeigen.

Anmerkung: Diese Task gilt nur für die 7063-CR1. Diese Verbindung ist für den Zugriff auf den Baseboard-Management-Controller (BMC) auf der HMC erforderlich.

Führen Sie die folgenden Schritte aus, um die BMC-Verbindung zu konfigurieren:

1. Klicken Sie im Navigationsbereich auf das Symbol **HMC-Verwaltung**  und wählen Sie anschließend **Konsoleneinstellungen** aus.
2. Klicken Sie im Inhaltsbereich auf **BMC/IPMI-Netzeinstellungen ändern**.
3. Wählen Sie den Verbindungsmodus (**DHCP** oder **Statisch**) aus.

   Geben Sie folgende Adressen an, wenn Sie den Modus **Statisch** auswählen:

   - **IP-Adresse**
   - **Teilnetzmaske**
   - **Gateway**
4. Klicken Sie auf **OK**.

Sie können die BMC-Netzverbindung auch über die Schnittstelle des Bootladeprogramms Petitboot konfigurieren. Weitere Informationen finden Sie unter IP-Adresse der Firmware konfigurieren.

IPv4-Adresse festlegen
Dieser Abschnitt enthält Informationen zur Definition Ihrer IPv4-Adresse auf der HMC.

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf das Symbol **HMC-Verwaltung**  und wählen Sie anschließend **Konsoleneinstellungen** aus.
2. Klicken Sie im Inhaltsbereich auf **Netzeinstellungen ändern**.
3. Klicken Sie auf die Registerkarte **LAN-Adapter**.
4. Wählen Sie den LAN-Adapter aus, mit dem Sie arbeiten möchten, und klicken Sie auf **Details**.
5. Klicken Sie auf die Registerkarte **Grundlegende Einstellungen**.
6. Wählen Sie eine IPv4-Adresse aus.
7. Wenn Sie "IP-Adresse angeben" ausgewählt haben, geben Sie die TCP/IP-Schnittstellenadresse und die Netzmaske der TCP/IP-Schnittstelle ein.
8. Klicken Sie auf **OK**.

IPv6-Adresse festlegen
Dieser Abschnitt enthält Informationen zur Definition Ihrer IPv6-Adresse auf der HMC.

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf das Symbol **HMC-Verwaltung**  und wählen Sie anschließend **Konsoleneinstellungen** aus.
2. Klicken Sie im Inhaltsbereich auf **Netzeinstellungen ändern**.
3. Klicken Sie auf die Registerkarte **LAN-Adapter**.
4. Wählen Sie den LAN-Adapter aus, mit dem Sie arbeiten möchten, und klicken Sie auf **Details**.
5. Klicken Sie auf die Registerkarte **IPv6-Einstellungen**.
6. Wählen Sie eine Option für die **Automatische Konfiguration** (Autoconfig) aus oder fügen Sie eine statische IP-Adresse hinzu.
7. Wenn Sie eine IP-Adresse hinzugefügt haben, geben Sie die IPv6-Adresse und die Präfixlänge ein und klicken Sie auf **OK**.
8. Klicken Sie auf **OK**.

Ausschließliche Verwendung von IPv6-Adressen
Hier erfahren Sie, wie Sie die HMC für die ausschließliche Verwendung von IPv6-Adressen konfigurieren.

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf das Symbol **HMC-Verwaltung**  und wählen Sie anschließend **Konsoleneinstellungen** aus.
2. Klicken Sie im Inhaltsbereich auf **Netzeinstellungen ändern**.
3. Klicken Sie auf die Registerkarte **LAN-Adapter**.
4. Wählen Sie den LAN-Adapter aus, mit dem Sie arbeiten möchten, und klicken Sie auf **Details**.
5. Wählen Sie **Keine IPv4-Adresse** aus.
6. Klicken Sie auf die Registerkarte **IPv6-Einstellungen**.
7. Wählen Sie **DHCPv6 zum Konfigurieren der IP-Einstellungen verwenden** aus oder fügen Sie eine statische IP-Adresse hinzu. Klicken Sie anschließend auf **OK**.

Nächste Schritte
Nachdem Sie auf **OK** geklickt haben, müssen Sie Ihre HMC erneut starten, damit diese Änderungen wirksam werden.

HMC-Firewalleinstellungen ändern
In einem offenen Netz wird der Zugriff von außerhalb Ihres Unternehmensnetzes in der Regel von einer Firewall kontrolliert. Die HMC verfügt auch über eine Firewall auf jedem Ihrer Ethernet-Adapter. Wenn die HMC über Remotezugriff gesteuert werden soll oder wenn andere Benutzer Remotezugriff erhalten sollen, ändern Sie die Firewalleinstellungen des Ethernet-Adapters auf der HMC, die an das offene Netz angeschlossen ist.

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um eine Firewall zu konfigurieren:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf das Symbol **HMC-Verwaltung**  und wählen Sie anschließend **Konsoleneinstellungen** aus.

2. Klicken Sie im Inhaltsbereich auf **Netzeinstellungen ändern**.
3. Klicken Sie auf die Registerkarte **LAN-Adapter**.
4. Wählen Sie den LAN-Adapter aus, mit dem Sie arbeiten möchten, und klicken Sie auf **Details**.
5. Klicken Sie auf die Registerkarte **Firewall**.
6. Mit einer der folgenden Methoden können Sie die Firewall von jeder IP-Adresse, die eine bestimmte Anwendung verwendet, passieren lassen oder Sie können eine oder mehrere IP-Adressen angeben:
   - Gehen Sie wie folgt vor, um die Firewall von jeder IP-Adresse, die eine bestimmte Anwendung verwendet, passieren zu lassen:
     a. Heben Sie die Anwendung im oberen Fenster hervor.
     b. Klicken Sie auf **Eingehende Daten zulassen**. Die Anwendung wird im unteren Fenster angezeigt. Dies bedeutet, dass sie ausgewählt wurde.
   - Gehen Sie wie folgt vor, um die Firewall von bestimmten IP-Adressen passieren zu lassen:
     a. Heben Sie im oberen Fenster eine Anwendung hervor.
     b. Klicken Sie auf **Eingehende Daten nach IP-Adresse zulassen**.
     c. Geben Sie im Fenster "Zulässige Hosts" die IP-Adresse und die Netzmaske ein.
     d. Klicken Sie auf **Hinzufügen** und auf **OK**.
7. Klicken Sie auf **OK**.

Fernzugriff auf eingeschränkte Shell aktivieren
Bei der Konfiguration einer Firewall können Sie Fernzugriff auf eingeschränkte Shell aktivieren.

Informationen zu diesem Vorgang
Führen Sie die folgenden Schritte aus, um Fernzugriff auf eingeschränkte Shell zu aktivieren:

Vorgehensweise
1. Klicken Sie im Navigationsbereich auf **HMC-Verwaltung**.
2. Klicken Sie auf **Ausführung von fernen Befehlen**.
3. Wählen Sie **Ausführung von fernen Befehlen über den ssh-Befehl** aus und klicken Sie dann auf **OK**.

Nächste Schritte
Jetzt ist Fernzugriff auf eingeschränkte Shell aktiviert.

Webfernzugriff aktivieren
Sie können für Ihre Hardware Management Console (HMC) Webfernzugriff aktivieren.

Informationen zu diesem Vorgang
Führen Sie die folgenden Schritte aus, um Webfernzugriff zu aktivieren:

Vorgehensweise
1. Klicken Sie im Navigationsbereich auf **HMC-Verwaltung**.
2. Klicken Sie auf **Fernen Betrieb**.
3. Wählen Sie **Aktivieren** aus und klicken Sie dann auf **OK**.

Nächste Schritte
Jetzt ist Webfernzugriff aktiviert.

Route-Eintrag als Standardgateway konfigurieren
In diesem Abschnitt wird die Konfiguration eines Route-Eintrags als Standardgateway beschrieben. Diese Task ist verfügbar, wenn Sie ein offenes Netz verwenden.

Vorbereitende Schritte

Führen Sie die folgenden Schritte aus, um einen Route-Eintrag als Standardgateway zu konfigurieren:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf das Symbol **HMC-Verwaltung**  und wählen Sie anschließend **Konsoleneinstellungen** aus.
2. Klicken Sie im Inhaltsbereich auf **Netzeinstellungen ändern**. Das Fenster "Netzeinstellungen anpassen" wird geöffnet.
3. Klicken Sie auf die Registerkarte **Routing**.
4. Geben Sie im Bereich für Standardgateway-Informationen die Gatewayadresse und die Gatewayeinheit des Route-Eintrags ein, der als Standardgateway verwendet werden soll.
5. Klicken Sie auf **OK**.

Domänennamensservices konfigurieren

Wenn Sie ein offenes Netz planen, konfigurieren Sie Domänennamensservices.

Informationen zu diesem Vorgang

Wenn Sie ein offenes Netz planen, konfigurieren Sie Domänennamensservices. Das DNS (Domain Name System) ist ein verteiltes Datenbanksystem zur Verwaltung von Hostnamen und deren zugehörigen IP-Adressen. Zur Konfiguration von Domänennamensservices gehört die Aktivierung von DNS und die Angabe der Suchreihenfolge für Domänensuffixe.

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf das Symbol **HMC-Verwaltung**  und wählen Sie anschließend **Konsoleneinstellungen** aus.
2. Klicken Sie im Inhaltsbereich auf **Netzeinstellungen ändern**. Das Fenster "Netzeinstellungen ändern" wird geöffnet.
3. Klicken Sie auf die Registerkarte **Namensservices**.
4. Wählen Sie **DNS aktiviert** aus, um das DNS zu aktivieren.
5. Geben Sie die Suchreihenfolge für DNS-Server und für Domänensuffixe ein und klicken Sie auf **Hinzufügen**.
6. Klicken Sie auf **OK**.

Domänensuffixe konfigurieren

Die Liste der Domänensuffixe wird zum Auflösen einer IP-Adresse verwendet, wobei mit dem ersten Eintrag in der Liste begonnen wird.

Informationen zu diesem Vorgang

Das Domänensuffix ist eine an einen Hostnamen angehängte Zeichenfolge, die zum Auflösen der zugehörigen IP-Adresse verwendet wird. Wenn z. B. der Hostname `meinname` nicht aufgelöst werden kann, aber die Zeichenfolge `meinort.meinefirma.com` ein Element der Domänensuffixtabelle ist, wird versucht, die Adresse `meinname.meinort.meinefirma.com` aufzulösen.

Führen Sie die folgenden Schritte aus, um einen Domänensuffixeintrag zu konfigurieren:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf das Symbol **HMC-Verwaltung**  und wählen Sie anschließend **Konsoleneinstellungen** aus.
2. Klicken Sie im Inhaltsbereich auf **Netzeinstellungen ändern**. Das Fenster "Netzeinstellungen anpassen" wird geöffnet.
3. Klicken Sie auf die Registerkarte **Namensservices**.
4. Geben Sie eine Zeichenfolge ein, die als Domänensuffixeintrag verwendet werden soll.
5. Klicken Sie auf **Hinzufügen**, um sie zur Liste hinzuzufügen.

HMC für die Verwendung von LDAP-Authentifizierung per Remotezugriff konfigurieren

Sie können Ihre Hardware Management Console (HMC) für die Verwendung von LDAP-Authentifizierung per Remotezugriff (LDAP = Lightweight Directory Access Protocol) konfigurieren.

Vorbereitende Schritte

Wenn sich ein Benutzer an der HMC anmeldet, wird eine Authentifizierung zuerst anhand einer lokalen Kennwortdatei ausgeführt. Wenn keine lokale Kennwortdatei vorhanden ist, kann die HMC eine Verbindung zu einem fernen LDAP-Server herstellen, um eine Authentifizierung vorzunehmen. Sie müssen Ihre HMC für die Verwendung der LDAP-Authentifizierung per Remotezugriff konfigurieren.

Anmerkung: Bevor Sie die HMC für die Verwendung der LDAP-Authentifizierung konfigurieren, müssen Sie sicherstellen, dass eine betriebsfähige Netzverbindung zwischen der HMC und den LDAP-Servern vorhanden ist. Weitere Informationen zur Konfiguration von HMC-Netzverbindungen finden Sie im Abschnitt „HMC-Netztypen konfigurieren” auf Seite 60.

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um Ihre HMC für die Verwendung von LDAP-Authentifizierung zu konfigurieren:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf das Symbol **Benutzer und Sicherheit**  und wählen Sie anschließend **System- und Konsolensicherheit** aus.
2. Wählen Sie im Inhaltsbereich **LDAP verwalten** aus. Das Fenster "LDAP-Serverdefinition" wird geöffnet.
3. Wählen Sie **LDAP aktivieren** aus.
4. Definieren Sie einen LDAP-Server, der für die Authentifizierung verwendet werden soll.
5. Definieren Sie das LDAP-Attribut, das zum Bestimmen des zu authentifizierenden Benutzers verwendet werden soll. Der Standardwert ist **uid**, Sie können jedoch Ihre eigenen Attribute verwenden.
6. Definieren Sie für den LDAP-Server die Baumstruktur für eindeutige Namen, auch als Suchbasis bekannt.
7. Klicken Sie auf **OK**.
8. Wenn ein Benutzer LDAP-Authentifizierung verwenden möchte, muss er sein Profil so konfigurieren, dass es LDAP-Authentifizierung per Remotezugriff anstelle von lokaler Authentifizierung verwendet.

HMC für die Verwendung von KDC-Servern für Kerberos-Authentifizierung per Remotezugriff konfigurieren

Sie können die HMC für die Verwendung von KDC-Servern (KDC = Key Distribution Center) für Kerberos-Authentifizierung per Remotezugriff konfigurieren.

Vorbereitende Schritte

Wenn sich ein Benutzer an der HMC anmeldet, wird eine Authentifizierung zuerst anhand einer lokalen Kennwortdatei ausgeführt. Wenn keine lokale Kennwortdatei vorhanden ist, kann die HMC eine Verbindung zu einem fernen Kerberos-Server herstellen, um eine Authentifizierung vorzunehmen. Sie müssen Ihre HMC für die Verwendung der Kerberos-Authentifizierung per Remotezugriff konfigurieren.

Anmerkung: Bevor Sie die HMC für die Verwendung der KDC-Server für Kerberos-Authentifizierung per Remotezugriff konfigurieren, müssen Sie sicherstellen, dass eine betriebsfähige Netzverbindung zwischen der HMC und den KDC-Servern vorhanden ist. Weitere Informationen zur Konfiguration von HMC-Netzverbindungen finden Sie im Abschnitt „HMC-Netztypen konfigurieren” auf Seite 60.

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um die HMC für die Verwendung von KDC-Servern für Kerberos-Authentifizierung per Remotezugriff zu konfigurieren:

Vorgehensweise

1. Aktivieren Sie den NTP-Service auf der HMC und legen Sie für die HMC und die KDC-Server Zeitsynchronisation mit demselben NTP-Server fest. Führen Sie die folgenden Schritte aus, um den NTP-Service auf der HMC zu aktivieren:
   a) Klicken Sie im Navigationsbereich auf das Symbol **HMC-Verwaltung**  und wählen Sie anschließend **Konsoleneinstellungen** aus.
   b) Wählen Sie im Inhaltsteilfenster **Datum und Uhrzeit ändern** aus.
   c) Wählen Sie die Registerkarte **NTP-Konfiguration** aus.
   d) Wählen Sie **NTP-Service auf dieser HMC aktivieren** aus.
   e) Klicken Sie auf **OK**.
2. Konfigurieren Sie das Profil jedes Benutzers einer fernen HMC für die Verwendung der Kerberos-Authentifizierung per Remotezugriff anstelle der lokalen Authentifizierung.
3. Optional: Sie können eine Serviceschlüsseldatei in diese HMC importieren. Die Serviceschlüsseldatei enthält den Hostprincipal, der die HMC für den KDC-Server bestimmt. Serviceschlüsseldateien werden auch als *Keytabs* bezeichnet. Führen Sie die folgenden Schritte aus, um eine Serviceschlüsseldatei in diese HMC zu importieren.
   a) Klicken Sie im Navigationsbereich auf das Symbol **Benutzer und Sicherheit**  und wählen Sie anschließend **System- und Konsolensicherheit** aus.
   b) Wählen Sie im Inhaltsteilfenster **KDC verwalten** aus.
   c) Wählen Sie **Aktionen > Serviceschlüssel importieren** aus. Das Fenster "Serviceschlüssel importieren" wird geöffnet.
   d) Geben Sie die Position der Serviceschlüsseldatei ein.
   e) Klicken Sie auf **OK**.
4. Fügen Sie einen neuen KDC-Server dieser HMC hinzu. Führen Sie dazu die folgenden Schritte aus:
   a) Klicken Sie im Navigationsbereich auf das Symbol **Benutzer und Sicherheit**  und wählen Sie anschließend **System- und Konsolensicherheit** aus.
   b) Wählen Sie im Inhaltsteilfenster **KDC verwalten** aus.
   c) Wählen Sie **Aktionen > KDC-Server hinzufügen** aus. Das Fenster "Serviceschlüssel importieren" wird geöffnet.
   d) Geben Sie den Realm und den Hostnamen oder die IP-Adresse des KDC-Servers ein.

e) Klicken Sie auf **OK**.

Lokale Konsole für die Fehlermeldung an Service und Support konfigurieren
Konfigurieren Sie diese HMC so, dass sie Fehler mittels LAN per Call-Home-Funktion melden kann.

HMC für die Verbindung zu Service und Support unter Verwendung des Installationsassistenten für die Call-Home-Funktion konfigurieren
Konfigurieren Sie die HMC als Call-Home-Server mithilfe des Installationsassistenten für die Call-Home-Funktion.

Vorbereitende Schritte
Hier wird beschrieben, wie die HMC als Call-Home-Server mit direkter (LAN-basierte) und indirekter Verbindung (SSL) zum Internet konfiguriert wird.

Bevor Sie mit dieser Task beginnen, muss Folgendes sichergestellt sein:

- Der Netzadministrator überprüft die Zulässigkeit der Konnektivität. Weitere Informationen finden Sie unter „HMC-Konfiguration vorbereiten" auf Seite 48.
- Wenn Sie Internetunterstützung über einen Proxy-Server konfigurieren, müssen die folgenden Informationen vorliegen:
  - Die IP-Adresse und der Anschluss des Proxy-Servers
  - Die Proxy-Authentifizierungsinformationen
- Der als **eth1** angegebene Adapter (derjenige, der als offenes Netz bestimmt wurde) wird verwendet. Weitere Informationen finden Sie unter „Netzeinstellungen auf der HMC auswählen" auf Seite 39.
- Die HMC wird über ein Ethernet-Kabel physisch an das LAN angeschlossen.

Um die HMC als Call-Home-Server unter Verwendung des Installationsassistenten für die Call-Home-Funktion zu konfigurieren, führen Sie die folgenden Schritte aus:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf das Symbol **Wartungsfähigkeit**  und wählen Sie anschließend **Service-Management** aus.
2. Klicken Sie im Inhaltsbereich auf **Installationsassistent für Call-Home-Funktion**. Der Assistent für Konnektivität und Call-Home-Server wird geöffnet. Befolgen Sie die Anweisungen des Assistenten zur Konfiguration der Call-Home-Funktion.

Lokale Konsole für die Fehlermeldung an Service und Support konfigurieren
Konfigurieren Sie diese HMC so, dass sie Fehler mittels LAN per Call-Home-Funktion melden kann.

HMC für die Kontaktaufnahme mit Service und Support über LAN-basiertes Internet und SSL konfigurieren
Hier wird beschrieben, wie die HMC als Call-Home-Server mit direkter (LAN-basierter) und indirekter Verbindung (SSL) zum Internet konfiguriert wird.

Vorbereitende Schritte

Bevor Sie mit dieser Task beginnen, muss Folgendes sichergestellt sein:

- Der Netzadministrator überprüft die Zulässigkeit der Konnektivität. Weitere Informationen finden Sie unter „HMC-Konfiguration vorbereiten" auf Seite 48.
- Die Kundenkontaktinformationen wurden konfiguriert. Überprüfen Sie die Kontaktinformationen, indem Sie die HMC-Schnittstelle aufrufen und auf **Wartungsfähigkeit >Service-Management > Kundendaten verwalten** klicken.
- Wenn Sie Internetunterstützung über einen Proxy-Server konfigurieren, müssen die folgenden Informationen vorliegen:

  - Die IP-Adresse und der Anschluss des Proxy-Servers
  - Die Proxy-Authentifizierungsinformationen
- Mindestens eine Schnittstelle zu einem öffentlichen Netz muss konfiguriert sein. Weitere Informationen finden Sie unter „Private und offene Netze in der HMC-Umgebung” auf Seite 41.
- Die HMC wird über ein Ethernet-Kabel physisch an das LAN angeschlossen.

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um die HMC als Call-Home-Server mit LAN-basiertem Internet und SSL zu konfigurieren:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf das Symbol **Wartungsfähigkeit**  und wählen Sie anschließend **Service-Management** aus.
2. Klicken Sie im Konnektivitätsbereich auf **Konnektivität abgehender Daten verwalten**. Das Fenster "Call-Home-Serverkonsolen" wird geöffnet.
3. Klicken Sie auf **Konfigurieren**.
4. Markieren Sie im Fenster "Einstellungen für Konnektivität nach außen" die Option zum Aktivieren des lokalen Systems als Call-Home-Server.
5. Akzeptieren Sie die Vereinbarung.
6. Wählen Sie im Fenster "Einstellungen für Konnektivität nach außen" die Seite **Internet** aus.
7. Markieren Sie das Feld **Bestehende Internetverbindung für den Dienst zulassen**.
8. Wenn Sie einen SSL-Proxy verwenden, markieren Sie das Feld **SSL-Proxy verwenden**.
9. Wenn Sie einen SSL-Proxy verwenden, geben Sie Adresse und Port des Proxys an. Diese Informationen erhalten Sie vom Netzadministrator.
10. Wenn Sie **SSL-Proxy verwenden** ausgewählt haben und für den Proxy eine Authentifizierung von Benutzer-ID und Kennwort erforderlich ist, markieren Sie das Feld **Mit dem SSL-Proxy authentifizieren**. Geben Sie die Benutzer-ID und das Kennwort ein. Benutzer-ID und Kennwort erhalten Sie vom Netzadministrator.
11. Wählen Sie das gewünschte **Internetprotokoll** aus.
12. Klicken Sie auf der Seite **Internet** auf **Testen**.
13. Klicken Sie im Fenster "Internet testen" auf **Start**.
14. Überprüfen Sie, ob der Test erfolgreich ist.
15. Klicken Sie im Fenster "Internet testen" auf **Abbrechen**.
16. Klicken Sie im Fenster "Einstellungen für Konnektivität nach außen" auf **OK**.

Vorhandene Call-Home-Server für die Verbindung zu Service und Support für diese HMC auswählen
Wählen Sie vorhandene HMC-Call-Home-Server aus, die von der HMC erkannt oder entdeckt werden, um Fehler zu melden.

Vorbereitende Schritte

Entdeckte oder erkannte HMCs sind HMCs, die als Call-Home-Server aktiviert sind und die sich entweder in demselben Teilnetz befinden oder dasselbe verwaltete System wie diese HMC verwalten.

Führen Sie die folgenden Schritte aus, um auszuwählen, dass eine erkannte HMC die Call-Home-Funktion ausführt, wenn diese HMC Fehler meldet:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf das Symbol **Wartungsfähigkeit**  und wählen Sie anschließend **Service-Management** aus.
2. Klicken Sie im Inhaltsbereich auf **Konnektivität nach außen verwalten**. Das Fenster "Call-Home-Serverkonsolen" wird geöffnet.
3. Klicken Sie auf **Erkannte Call-Home-Serverkonsolen verwenden**. Die HMC zeigt die IP-Adresse oder den Hostnamen der HMCs an, die für die Call-Home-Funktion konfiguriert wurden.
4. Klicken Sie auf **OK**.

Ergebnisse

Sie können auch bestehende HMC-Call-Home-Server, die sich in einem anderen Teilnetz befinden, manuell hinzufügen. Wählen Sie die IP-Adresse oder den Hostnamen der HMC aus, die für die Call-Home-Funktion konfiguriert ist, und klicken Sie auf **Hinzufügen** und dann auf **OK**.

Prüfen, ob die Verbindung zu Service und Support funktioniert
Testen Sie die Problemmeldung, um sicherzustellen, dass die Verbindung zu Service und Support funktioniert.

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um zu prüfen, ob die Call-Home-Konfiguration funktioniert:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf das Symbol **Wartungsfähigkeit**  und wählen Sie anschließend **Service-Management** aus.
2. Klicken Sie im Inhaltsbereich auf **Ereignis erstellen**.
3. Wählen Sie **Automatische Problemmeldung testen** und geben Sie einen Kommentar ein.
4. Klicken Sie auf **Service anfordern**. Warten Sie einige Minuten, bis die Anforderung gesendet wurde.
5. Wählen Sie im Fenster "Service-Management" **Ereignisse verwalten** aus.
6. Wählen Sie **Alle offenen Probleme** aus.
7. Überprüfen Sie, ob ein PMH-Ereignis und eine -Nummer der von Ihnen geöffneten Fehlernummer zugeordnet ist.
8. Wählen Sie dieses Ereignis aus und klicken Sie auf **Schließen**.
9. Geben Sie im Fenster **Schließen** Ihren Namen und einen kurzen Kommentar ein.

Benutzer zum Anzeigen erfasster Systemdaten berechtigen
Sie müssen Benutzer zum Anzeigen von Daten über Ihre Systeme berechtigen.

Vorbereitende Schritte

Bevor Sie Benutzer zum Anzeigen erfasster Systemdaten berechtigen, müssen Sie eine IBM ID abrufen. Weitere Informationen über das Abrufen einer IBM ID finden Sie unter „Arbeitsblatt zur Konfiguration bei der Installationsvorbereitung für die HMC” auf Seite 49.

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um Benutzer zum Anzeigen von erfassten Systemdaten zu berechtigen:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf das Symbol **Wartungsfähigkeit**  und wählen Sie anschließend **Service-Management** aus.
2. Wählen Sie im Inhaltsbereich **Benutzer autorisieren** aus.
3. Geben Sie Ihre IBM ID ein.
4. Klicken Sie auf **OK**.

Serviceinformationen übertragen
Sie können Informationen sofort zum Service-Provider übertragen oder das regelmäßige Versenden der Informationen planen.

Vorbereitende Schritte
IBM stellt angepasste Webfunktionen bereit, die von IBM Electronic Service Agent gesammelte Informationen verwenden. Damit Sie diese Funktionen verwenden können, müssen Sie sich zunächst auf der IBM Registrierungswebsite unter http://www.ibm.com/account/profile registrieren. Um Benutzer für die Verwendung der Informationen des Electronic Service Agent für die Anpassung der Webfunktionen zu autorisieren, lesen Sie den Abschnitt „Benutzer zum Anzeigen erfasster Systemdaten berechtigen" auf Seite 74. Weitere Informationen über die Vorteile der Registrierung einer IBM ID für Ihre Systeme, finden Sie unter http://www.ibm.com/support/electronic.

Anmerkung: Sie sollten Service-Provider-Informationen sofort nach der Installation und Konfiguration der HMC übertragen.

Informationen zu diesem Vorgang
Führen Sie die folgenden Schritte aus, um Serviceinformationen zu übertragen:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf das Symbol **Wartungsfähigkeit**  und wählen Sie anschließend **Service-Management** aus.
2. Klicken Sie im Inhaltsbereich auf **Serviceinformationen übertragen**.
3. Führen Sie die Tasks im Fenster **Serviceinformationen übertragen** aus und klicken Sie auf **OK**.

Ereignismanager für die Call-Home-Funktion konfigurieren
Hier wird beschrieben, wie Sie die Task des Ereignismanagers für die Call-Home-Funktion konfigurieren. Sie können über diese Task alle Daten überwachen und freigeben, die von einer HMC an IBM übertragen werden.

Der Ereignismanager für den Modus der Call-Home-Funktion (aktiviert oder inaktiviert) wird über die Befehlszeilenschnittstelle der HMC festgelegt. Durch die Aktivierung der Task des Ereignismanagers für die Call-Home-Funktion wird die automatische Call-Home-Funktion für Ereignisse blockiert, wenn diese auf der HMC auftreten. Um zu verhindern, dass die Call-Home-Funktion bei Ereignissen ohne Genehmigung eingesetzt wird, muss diese im Ereignismanager auf allen HMCs aktiviert sein, die in dieser Umgebung ausgeführt werden.

Führen Sie den folgenden Befehl aus, um die Task des Ereignismanagers für die Call-Home-Funktion zu aktivieren oder zu inaktivieren:

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

[--help]

Anmerkung: Durch die Aktivierung des Ereignismanagers für die Call-Home-Funktion werden Call-Home-Ereignisse so lange aufbewahrt, bis sie für die Call-Home-Funktion genehmigt wurden. Wenn Sie den Ereignismanager für die Call-Home-Funktion inaktivieren, wird die Call-Home-Funktion nicht automatisch aktiviert. Dadurch wird ein unbeabsichtigtes Call Home von Daten zurück an IBM verhindert. Wählen Sie eine der folgenden Befehlsoptionen aus, um die erforderliche Konfiguration einzurichten:

- Zur Aktivierung des Ereignismanagers für die Call-Home-Funktion: **chhmc -c emch -s enable**
- Zur Inaktivierung des Ereignismanagers für die Call-Home-Funktion und zur erneuten Aktivierung der automatischen Call-Home-Funktion: **chhmc -c emch -s disable --callhome enable**
- Zur Inaktivierung der Ereignismanagers für die Call-Home-Funktion und zur erneuten Aktivierung der automatischen Call-Home-Funktion: **chhmc -c emch -s disable --callhome disable**

Stellen Sie sicher, dass die HMC mit anderen in dieser Umgebung bereitgestellten HMCs kommunizieren kann. Der Ereignismanager für die Call-Home-Funktion verfügt über eine Testverbindungsfunktion, wenn eine HMC registriert wird.

Sie können die HMC mit dem Ereignismanager für die Call-Home-Funktion registrieren. Nach der Registrierung der HMC fragt der Ereignismanager ab, ob die HMC Ereignisse enthält, die über die Call-Home-Funktion an IBM zurückgesendet werden sollen. Der Ereignismanager zeigt an, welche Daten an IBM zurückgesendet werden und gibt diese Ereignisse frei. Nach der Freigabe benachrichtigt der Ereignismanager die registrierte HMC darüber, dass sie mit dem Call-Home-Vorgang fortfahren kann.

Die Task des Ereignismanagers für die Call-Home-Funktion kann von jeder HMC oder mehreren HMCs ausgeführt werden. Führen Sie die folgenden Schritte aus, um eine Managementkonsole in der Task des Ereignismanagers für die Call-Home-Funktion zu registrieren:

1. Klicken Sie im Navigationsbereich auf das Symbol **Wartungsfähigkeit**  und wählen Sie anschließend **Ereignismanager für Call-Home-Funktion** aus.
2. Klicken Sie im Fenster **Ereignismanager für Call-Home-Funktion** auf **Konsolen verwalten**.
3. Klicken Sie im Fenster **Registrierte Konsolen verwalten** auf **Konsole hinzufügen**, um Informationen für die Registrierung einer Managementkonsole im Ereignismanager für die Call-Home-Funktion einzugeben.
4. Klicken Sie auf **OK**, um die Änderungen an der Liste der registrierten Managementkonsole festzuschreiben.

Anmerkung: Der Ereignismanager für die Call-Home-Funktion kann im inaktivierten Modus des Ereignismanagers verwendet werden. Sie können die HMC dann noch registrieren und Ereignisse im Ereignismanager anzeigen, der Ereignismanager steuert jedoch nicht, wenn die Ereignisse über die Call-Home-Funktion zurückgesendet werden.

Kennwörter für das verwaltete System festlegen

Sie müssen sowohl für Ihren Server als auch für Advanced System Management (ASM) Kennwörter festlegen. Im Folgenden erhalten Sie weitere Informationen über die Verwendung der HMC-Schnittstelle bei der Festlegung dieser Kennwörter.

Vorbereitende Schritte

Wenn Sie die Nachricht `Authentifizierung anstehend` erhalten haben, werden Sie von der HMC aufgefordert, die Kennwörter für das verwaltete System festzulegen.

Informationen zu diesem Vorgang

Wenn Sie die Nachricht "Authentifizierung anstehend" nicht erhalten haben, führen Sie die folgenden Schritte aus, um die Kennwörter für das verwaltete System festzulegen.

Serverkennwort aktualisieren

Vorbereitende Schritte

Führen Sie die folgenden Schritte aus, um das Serverkennwort zu aktualisieren:

Vorgehensweise

1. Wählen Sie im Navigationsbereich das verwaltete System aus, klicken Sie auf das Symbol **Benutzer und Sicherheit**  und wählen Sie anschließend **Benutzer und Rollen** aus.
2. Klicken Sie auf **Kennwort ändern**. Das Fenster "Kennwort aktualisieren" wird geöffnet.
3. Geben Sie erforderlichen Informationen ein und klicken Sie auf **OK**.

Allgemeines ASM-Kennwort (Advanced System Management) aktualisieren

Vorbereitende Schritte

Anmerkung: Das Standardkennwort für die allgemeine Benutzer-ID ist `general`, das Standardkennwort für die Administrator-ID ist `admin`.

Führen Sie die folgenden Schritte aus, um das allgemeine ASM-Kennwort zu aktualisieren:

Vorgehensweise

1. Wählen Sie im Navigationsbereich der HMC das verwaltete System aus.
2. Klicken Sie im Bereich "Tasks" auf **Vorgänge**.
3. Klicken Sie auf **ASM (Advanced System Management)**. Das Fenster "ASM-Schnittstelle starten" wird geöffnet.
4. Wählen Sie eine IP-Adresse des Serviceprozessors aus und klicken Sie auf **OK**. Die ASM-Schnittstelle wird geöffnet.
5. Geben Sie in der ASMI-Eingangsanzeige Ihre Benutzer-ID und Ihr Kennwort an und klicken Sie auf **Anmeldung**.
6. Erweitern Sie im Navigationsbereich **Anmeldeprofil**.
7. Wählen Sie **Kennwort ändern** aus.
8. Geben Sie die erforderlichen Informationen an und klicken Sie auf **Weiter**.

ASM-Administratorkennwort (Advanced System Management) zurücksetzen

Vorbereitende Schritte

Kontaktieren Sie einen autorisierter Service-Provider, um das Administratorkennwort zurückzusetzen.

Verbindung zwischen HMC und verwaltetem System testen

Hier erfahren Sie, wie Sie prüfen, ob Sie ordnungsgemäß mit dem Netz verbunden sind.

Informationen zu diesem Vorgang

Zum Testen der Netzkonnektivität müssen Sie einer der folgenden Berechtigungsklassen angehören:

- Superadministrator
- Ansprechpartner

Zum Testen der Verbindung zwischen der HMC und dem verwalteten System müssen Sie die folgenden Schritte ausführen:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf das Symbol **HMC-Verwaltung**  und wählen Sie anschließend **Konsoleneinstellungen** aus.
2. Klicken Sie im Inhaltsbereich auf **Netzverbindung testen**.
3. Geben Sie auf der Registerkarte "Ping" den Hostnamen oder die IP-Adresse eines Systems ein, zu dem Sie eine Verbindung herstellen möchten. Geben Sie den Gateway an, um ein offenes Netz zu testen. Klicken Sie auf **Ping**.

Ergebnisse

Wenn Sie keine logischen Partitionen erstellt haben, können Sie die Adressen nicht mit Ping überprüfen. Mit der HMC können Sie logische Partitionen auf Ihrem Server erstellen. Weitere Informationen finden Sie unter Logische Partitionierung.

Lesen Sie „HMC-Netzverbindungen” auf Seite 39, wenn Sie wissen möchten, wie die HMC in einem Netz verwendet werden kann.

Weitere Informationen zum Konfigurieren der HMC für die Verbindung mit einem Netz finden Sie unter „HMC mithilfe der Menüs konfigurieren ” auf Seite 57.

Nach der Konfiguration auszuführende Schritte

Nachdem Sie die HMC installiert und konfiguriert haben, können Sie bei Bedarf HMC-Daten sichern.

Daten der Managementkonsole sichern

Diese Task sichert (oder archiviert) die Daten, die auf Ihrer HMC-Festplatte gespeichert sind und die für die Unterstützung von HMC-Operationen von entscheidender Bedeutung sind.

Vorbereitende Schritte

Auf dem fernen System muss NFS (Network File System) oder SSH (Secure Shell) konfiguriert sein und der Zugriff auf dieses Netz muss von der HMC aus möglich sein. Damit diese Task vollständig ausgeführt wird, müssen Sie die HMC beenden und anschließend einen Warmstart durchführen. Führen Sie diese Tasks nur mit der HMC aus.

Informationen zu diesem Vorgang

Zum Sichern des HMC-Festplattenlaufwerks auf einem fernen System müssen Sie einer der folgenden Berechtigungsklassen angehören:

- Superadministrator
- Bediener
- Ansprechpartner

Sichern Sie die HMC-Daten, nachdem Änderungen an der HMC oder den Informationen zu logischen Partitionen vorgenommen wurden.

Die HMC-Daten, die auf dem HMC-Festplattenlaufwerk gespeichert sind, können auf einer DVD-RAM auf einem lokalen System oder auf einem fernen System, das an das HMC-Dateisystem angehängt ist (zum Beispiel NFS) gespeichert oder über FTP an einen fernen Standort gesendet werden.

Anmerkung: Für HMC-Modell 7063-CR1 können Sie ein externes USB-DVD-Laufwerk anschließen.

Mit der HMC können Sie alle wichtigen Daten sichern, wie z. B.:

- Dateien mit Benutzervorgaben
- Benutzerinformationen

- HMC-Plattformkonfigurationsdateien
- HMC-Protokolldateien
- HMC-Aktualisierungen durch Installation von Fehlerberichtigungen

Um das HMC-Festplattenlaufwerk auf einem fernen System zu sichern, führen Sie die folgenden Schritte aus:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf das Symbol **HMC-Verwaltung**  und wählen Sie anschließend **Konsolenverwaltung** aus.
2. Klicken Sie im Inhaltsbereich auf **Daten der Managementkonsole sichern**.
3. Wählen Sie im Fenster **Daten der Managementkonsole sichern** die Archivierungsoption aus, die Sie ausführen möchten.
4. Klicken Sie auf **Weiter** und befolgen Sie die Anweisungen zur ausgewählten Option.
5. Klicken Sie auf **OK**, um mit dem Backup-Prozess fortzufahren.

Aktualisierung, Upgrade und Migration des HMC-Maschinencodes

Updates (Aktualisierungen) und Upgrades werden in regelmäßigen Abständen für die HMC freigegeben, um neue Funktionalität hinzuzufügen oder vorhandene Funktionen zu verbessern. Weitere Informationen über die Unterschiede zwischen Aktualisierung, Upgrade und Migration des HMC-Maschinencodes. Außerdem erfahren Sie, wie Sie eine Aktualisierung, ein Upgrade oder eine Migration des HMC-Maschinencodes ausführen können.

Nach Abschluss aller Tasks wird die HMC neu gebootet, die Partitionen jedoch nicht.

HMC-Code aktualisieren
Eine vorhandene HMC-Version wird gepflegt.

Es ist dabei nicht erforderlich, dass die Task **Upgradedaten speichern** ausgeführt wird.

Upgrade des HMC-Codes durchführen
HMC-Software wird durch ein neues Release oder eine neue Fixversion desselben Programms ersetzt.

Dabei müssen Sie über Wiederherstellungsdatenträger booten.

HMC-Code migrieren
HMC-Daten werden von einer HMC-Version in eine andere versetzt.

Eine Migration ist eine Art von Upgrade.

Anmerkung: Für HMC-Modell 7063-CR1 können Sie ein externes USB-DVD-Laufwerk anschließen.

Version und Release Ihres HMC-Maschinencodes bestimmen

Dieser Abschnitt enthält Informationen zum Anzeigen der Version und des Releases des HMC-Maschinencodes.

Informationen zu diesem Vorgang

Die Version des Maschinencodes auf der HMC bestimmt die verfügbaren Funktionen, einschließlich Server-Firmware-Parallelwartung und funktionale Erweiterungen für das Upgrade auf ein neues Release.

Führen Sie die folgenden Schritte aus, um Version und Release der HMC-Maschinencodeversion anzuzeigen:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf das Symbol **HMC-Verwaltung**  und wählen Sie anschließend **Konsolenverwaltung** aus.
2. Klicken Sie im Inhaltsbereich auf **Hardware Management Console aktualisieren**.
3. Sehen Sie sich im neuen Fenster die Informationen an, die unter der Überschrift **Informationen zum aktuellen HMC-Treiber** angezeigt werden, und notieren Sie die Informationen: HMC-Version, Release, Wartungsstufe, Buildstufe und Basisversion.

Updates des Maschinencodes für eine HMC mit einer Internetverbindung abrufen und installieren

Dieser Abschnitt enthält Informationen zum Abrufen von Updates für den HMC-Maschinencode, wenn die HMC über eine Internetverbindung verfügt.

Informationen zu diesem Vorgang

Führen Sie alle Schritte aus, um Updates für den HMC-Maschinencode abzurufen.

Schritt 1. Internetverbindung sicherstellen

Informationen zu diesem Vorgang

Damit Updates aus dem System oder von der Website für Service und Support auf Ihre HMC oder Ihren Server heruntergeladen werden können, benötigen Sie eine der folgenden Verbindungen:

- SSL-Konnektivität mit oder ohne SSL-Proxy
- Internet-VPN

Gehen Sie wie folgt vor, um das Vorhandensein einer Internetverbindung sicherzustellen:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf das Symbol **Wartungsfähigkeit**  und wählen Sie anschließend **Service-Management** aus.
2. Klicken Sie im Inhaltsbereich auf **Konnektivität nach außen verwalten**.
3. Wählen Sie die Registerkarte für die Art der Konnektivität abgehender Daten, die Sie für Ihre HMC wählen (Internet-VPN oder SSL-Konnektivität).

   Anmerkung: Besteht keine Verbindung zu Service und Support, konfigurieren Sie die Serviceverbindung, bevor Sie diese Prozedur fortsetzen. Informationen zur Konfiguration einer Verbindung zu Service und Support von IBM finden Sie im Abschnitt "Server für die Verbindung zu Service und Support konfigurieren".
4. Klicken Sie auf **Testen**.
5. Überprüfen Sie, ob der Test erfolgreich ist.

   Ist der Test nicht erfolgreich, müssen Sie eine Fehlerbehebung für Ihre Verbindung ausführen, bevor Sie diese Prozedur fortsetzen. Alternativ können Sie das Update auf DVD besorgen.

   Anmerkung: Für HMC-Modell 7063-CR1 können Sie ein externes USB-DVD-Laufwerk anschließen.
6. Fahren Sie mit „Schritt 2. Vorhandene HMC-Maschinencodeversion anzeigen” auf Seite 81 fort.

Schritt 2. Vorhandene HMC-Maschinencodeversion anzeigen

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um die vorhandene HMC-Maschinencodeversion anzuzeigen:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf das Symbol **HMC-Verwaltung**  und wählen Sie anschließend **Konsolenverwaltung** aus.
2. Klicken Sie im Inhaltsbereich auf **Hardware Management Console aktualisieren**.
3. Sehen Sie sich im neuen Fenster die Informationen an, die unter der Überschrift zu aktuellen HMC-Treiberinformationen angezeigt werden (einschließlich HMC-Version, Release, Programmfix, Erstellungsstufe und Basisversion), und notieren Sie die Informationen.
4. Fahren Sie mit „Schritt 3. Verfügbare HMC-Maschinencodeversionen anzeigen" auf Seite 81 fort.

Schritt 3. Verfügbare HMC-Maschinencodeversionen anzeigen

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um die verfügbaren HMC-Maschinencodeversionen anzuzeigen:

Vorgehensweise

1. Rufen Sie von einem Computer oder Server mit Internetverbindung die Website http://www.ibm.com/eserver/support/fixes auf.
2. Wählen Sie die entsprechende Produktfamilie aus der Liste für die Produktfamilie aus.
3. Wählen Sie **Hardware Management Console** in der Liste für Produkt- bzw. Fixtypen aus.
4. Klicken Sie auf **Weiter**.

   Die Site für die Hardware Management Console wird angezeigt.
5. Blättern Sie zum Versionsstand Ihrer HMC, um die verfügbaren HMC-Versionen anzuzeigen.

   Anmerkung: Sie können sich auch an Service und Support wenden.
6. Fahren Sie mit „Schritt 4. Update für HMC-Maschinencode installieren" auf Seite 81 fort.

Schritt 4. Update für HMC-Maschinencode installieren

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um das Update für HMC-Maschinencode zu installieren:

Vorgehensweise

1. Sichern Sie kritische Konsolinformationen auf Ihrer HMC, bevor Sie die Updates für den HMC-Maschinencode installieren.

   Anweisungen dazu finden Sie unter „Daten der Managementkonsole sichern" auf Seite 78. Fahren Sie anschließend mit dem nächsten Schritt fort.
2. Klicken Sie im Navigationsbereich auf das Symbol **HMC-Verwaltung**  und wählen Sie anschließend **Konsolenverwaltung** aus.
3. Klicken Sie im Inhaltsbereich auf **Hardware Management Console aktualisieren**. Der Assistent zur Installation der Fehlerberichtigung wird geöffnet.

4. Befolgen Sie die Anweisungen des Assistenten zur Installation des Updates.
5. Führen Sie für die HMC einen Systemabschluss und anschließend einen Neustart durch, damit die Aktualisierungen wirksam werden.
6. Klicken Sie auf **Melden Sie sich bei der Hardware Management Console-Webanwendung an und starten Sie diese**.
7. Melden Sie sich an der HMC-Schnittstelle an.

Schritt 5. Überprüfen, ob das Update für den HMC-Maschinencode erfolgreich installiert wurde

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um zu überprüfen, ob das Update für den HMC-Maschinencode ordnungsgemäß installiert wurde:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf das Symbol **HMC-Verwaltung**  und wählen Sie anschließend **Konsolenverwaltung** aus.
2. Klicken Sie im Inhaltsbereich auf **Hardware Management Console aktualisieren**.
3. Sehen Sie sich im neuen Fenster die Informationen an, die unter der Überschrift zu aktuellen HMC-Treiberinformationen angezeigt werden (einschließlich HMC-Version, Release, Programmfix, Erstellungsstufe und Basisversion), und notieren Sie die Informationen.
4. Überprüfen Sie, ob die Version und das Release dem installierten Update entsprechen.
5. Gehen Sie wie folgt vor, wenn die angezeigte Codeversion nicht mit der installierten Version übereinstimmt:
   a. Wählen Sie die Netzverbindung der HMC aus.
   b. Wiederholen Sie die Firmware-Aktualisierung mit einem anderen Repository.
   c. Wenn das Problem bestehen bleibt, wenden Sie sich an die nächste Unterstützungsstufe.

Updates für den HMC-Maschinencode mit DVD oder mit einem FTP-Server abrufen und installieren

Dieser Abschnitt enthält Informationen zum Abrufen von Updates für die Hardware Management Console (HMC) mit DVD oder mit einem FTP-Server.

Informationen zu diesem Vorgang

Führen Sie alle Schritte aus, um Updates für den HMC-Maschinencode abzurufen.

Anmerkung: Für HMC-Modell 7063-CR1 können Sie ein externes USB-DVD-Laufwerk anschließen.

Schritt 1. Vorhandene HMC-Maschinencodeversion anzeigen

Vorbereitende Schritte

Führen Sie die folgenden Schritte aus, um die vorhandene HMC-Maschinencodeversion anzuzeigen:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf das Symbol **HMC-Verwaltung**  und wählen Sie anschließend **Konsolenverwaltung** aus.

2. Klicken Sie im Inhaltsbereich auf **Hardware Management Console aktualisieren**.
3. Sehen Sie sich im neuen Fenster die Informationen an, die unter der Überschrift zu aktuellen HMC-Treiberinformationen angezeigt werden (einschließlich HMC-Version, Release, Programmfix, Erstellungsstufe und Basisversion), und notieren Sie die Informationen.
4. Fahren Sie mit „Schritt 2. Verfügbare HMC-Maschinencodeversionen anzeigen" auf Seite 83 fort.

Schritt 2. Verfügbare HMC-Maschinencodeversionen anzeigen

Vorbereitende Schritte

Führen Sie die folgenden Schritte aus, um die verfügbaren HMC-Maschinencodeversionen anzuzeigen:

Informationen zu diesem Vorgang

Vorgehensweise

1. Rufen Sie von einem Computer oder Server mit Internetverbindung die Website Fix Central auf.
2. Blättern Sie zum Versionsstand Ihrer HMC, um die verfügbaren HMC-Versionen anzuzeigen.

   Anmerkung: Sie können sich auch an Service und Support von IBM wenden.
3. Fahren Sie mit „Schritt 3. Update für HMC-Maschinencode abrufen" auf Seite 83 fort.

Schritt 3. Update für HMC-Maschinencode abrufen

Vorbereitende Schritte

Führen Sie die folgenden Schritte aus, um das Update für HMC-Maschinencode zu erhalten:

Informationen zu diesem Vorgang

Sie können das Update für den HMC-Maschinencode über die Fix Central-Website bestellen, sich an Service und Support wenden oder ihn auf einen FTP-Server herunterladen.

Update für den HMC-Maschinencode über die Fix Central-Website bestellen

1. Rufen Sie von einem Computer oder Server mit Internetverbindung die Website Fix Central auf.
2. Wählen Sie unter den unterstützten HMC-Produkten die neueste HMC-Version aus.
3. Blättern Sie zum Bereich File name(s) / Package und suchen Sie das Update, das Sie bestellen möchten.
4. Wählen Sie **Go** in der Spalte 'Order' aus.
5. Klicken Sie auf **Continue**, um eine Anmeldung mit Ihrer IBM ID auszuführen.
6. Befolgen Sie die angezeigten Bedienerführungen, um Ihre Bestellung zu übergeben.

Update für den HMC-Maschinencode auf austauschbare Datenträger herunterladen

1. Rufen Sie von einem Computer oder Server mit Internetverbindung die Website Fix Central auf.
2. Wählen Sie unter den unterstützten HMC-Produkten die neueste HMC-Version aus.
3. Blättern Sie zum Bereich File name(s) / Package und suchen Sie das Update, das Sie herunterladen möchten.
4. Klicken Sie auf das gewünschte Update.
5. Akzeptieren Sie die Lizenzvereinbarung und speichern Sie das Update auf den austauschbaren Datenträger.

Nächste Schritte

Wenn Sie fertig sind, fahren Sie mit „Schritt 4. Update für HMC-Maschinencode installieren” auf Seite 84 fort.

Schritt 4. Update für HMC-Maschinencode installieren

Vorbereitende Schritte

Führen Sie die folgenden Schritte aus, um das Update für HMC-Maschinencode zu installieren:

Vorgehensweise

1. Sichern Sie die HMC-Daten, bevor Sie die Updates für den HMC-Maschinencode installieren. Weitere Informationen finden Sie unter „Daten der Managementkonsole sichern” auf Seite 78.
2. Wenn Sie das Update auf DVD-RAM kopiert oder erstellt haben, legen Sie diese in das DVD-Laufwerk der HMC ein. Wenn Sie das Update auf einer USB-Speichereinheit erhalten oder erstellt haben, legen Sie diese ein.
3. Sichern Sie kritische Konsolinformationen auf Ihrer HMC, bevor Sie die Updates für den HMC-Maschinencode installieren.

   Anweisungen dazu finden Sie unter „Daten der Managementkonsole sichern” auf Seite 78. Fahren Sie anschließend mit dem nächsten Schritt fort.
4. Klicken Sie im Navigationsbereich auf das Symbol **HMC-Verwaltung**  und wählen Sie anschließend **Konsolenverwaltung** aus.
5. Klicken Sie im Inhaltsbereich auf **Hardware Management Console aktualisieren**. Der Assistent zur Installation der Fehlerberichtigung wird geöffnet.
6. Befolgen Sie die Anweisungen des Assistenten zur Installation des Updates.
7. Führen Sie einen Systemabschluss und einen Neustart durch und melden Sie sich dann wieder an der HMC an, damit das Update wirksam wird.
8. Fahren Sie mit „Schritt 5. Überprüfen, ob das Update für den HMC-Maschinencode erfolgreich installiert wurde” auf Seite 84 fort.

Schritt 5. Überprüfen, ob das Update für den HMC-Maschinencode erfolgreich installiert wurde

Vorbereitende Schritte

Führen Sie die folgenden Schritte aus, um zu überprüfen, ob das Update für den HMC-Maschinencode erfolgreich installiert wurde:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf das Symbol **HMC-Verwaltung**  und wählen Sie anschließend **Konsolenverwaltung** aus.
2. Klicken Sie im Inhaltsbereich auf **Hardware Management Console aktualisieren**.
3. Sehen Sie sich im neuen Fenster die Informationen an, die unter der Überschrift zu aktuellen HMC-Treiberinformationen angezeigt werden (einschließlich HMC-Version, Release, Programmfix, Erstellungsstufe und Basisversion), und notieren Sie die Informationen.
4. Überprüfen Sie, ob die Version und das Release dem installierten Update entsprechen.
5. Führen Sie die folgenden Schritte aus, wenn die angezeigte Codeversion nicht mit der installierten Version übereinstimmt:

a. Wiederholen Sie das Update für den Maschinencode. Wenn Sie eine DVD für diese Prozedur erstellt haben, verwenden Sie einen neuen Datenträger.
b. Wenn das Problem bestehen bleibt, wenden Sie sich an die nächste Unterstützungsstufe.

Upgrade der HMC-Software durchführen

Dieser Abschnitt enthält Informationen darüber, wie ein Upgrade der Software auf einer HMC von einem Release auf das nächste Release durchgeführt wird, während die HMC-Konfigurationsdaten beibehalten werden.

Informationen zu diesem Vorgang

Führen Sie alle Schritte aus, um ein Upgrade des Maschinencodes auf einer HMC durchzuführen.

Anmerkung: Für die HMC-Modelle 7063-CR1 und 7063-CR2 können Sie ein externes USB-DVD-Laufwerk anschließen.

Schritt 1. Upgrade besorgen

Informationen zu diesem Vorgang

Sie können das Upgrade für den HMC-Maschinencode über die Fix Central-Website bestellen.

Führen Sie die folgenden Schritte aus, um das Upgrade über die Fix Central-Website zu erhalten:

Vorgehensweise

1. Rufen Sie von einem Computer oder Server mit Internetverbindung die Website für die Hardware Management Console unter http://www-933.ibm.com/support/fixcentral/ auf.
2. Klicken Sie auf **Weiter**.

   Die Site für die Hardware Management Console wird angezeigt.
3. Navigieren Sie zu der gewünschten HMC-Version.
4. Suchen Sie den Abschnitt für Download und Bestellung.

   Anmerkung: Ist keine Internetverbindung vorhanden, wenden Sie sich an IBM Service und Support, um das Upgrade auf DVD zu bestellen.
5. Befolgen Sie die angezeigten Bedienerführungen, um Ihre Bestellung zu übergeben.
6. Nachdem Sie das Upgrade erhalten haben, fahren Sie mit „Schritt 2. Vorhandene HMC-Maschinencodeversion anzeigen” auf Seite 85 fort.

Schritt 2. Vorhandene HMC-Maschinencodeversion anzeigen

Informationen zu diesem Vorgang

Gehen Sie wie folgt vor, um die vorhandene Version des Maschinencodes auf einer HMC zu bestimmen:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf das Symbol **HMC-Verwaltung**  und wählen Sie anschließend **Konsolenverwaltung** aus. Klicken Sie im Navigationsbereich auf **Aktualisierungen**.
2. Klicken Sie im Inhaltsbereich auf **Hardware Management Console aktualisieren**.
3. Sehen Sie sich im neuen Fenster die Informationen an, die unter der Überschrift zu aktuellen HMC-Treiberinformationen angezeigt werden (einschließlich HMC-Version, Release, Programmfix, Erstellungsstufe und Basisversion), und notieren Sie die Informationen.
4. Fahren Sie mit „Schritt 3. Profildaten des verwalteten Systems sichern” auf Seite 86 fort.

Schritt 3. Profildaten des verwalteten Systems sichern

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um die Profildaten des verwalteten Systems zu sichern:

Vorgehensweise

1. Wählen Sie das System aus, auf dem die Profildaten gespeichert werden sollen.
2. Klicken Sie auf **Aktionen** > **Alle Aktionen anzeigen** > **Legacy** > **Partitionsdaten verwalten** > **Sichern**.
3. Geben Sie einen Namen für die Sicherungsdatei ein und notieren Sie diese Informationen.
4. Klicken Sie auf **OK**.
5. Wiederholen Sie diese Schritte für jedes System.
6. Fahren Sie mit „Schritt 4. HMC-Daten sichern” auf Seite 86 fort.

Schritt 4. HMC-Daten sichern

Informationen zu diesem Vorgang

Sichern Sie HMC-Daten, bevor Sie eine neue Version der HMC-Software installieren, so dass die vorherige Version wieder hergestellt werden kann, wenn beim Upgrade der Software ein Problem auftritt. Verwenden Sie diese kritischen Konsolendaten nicht, nachdem ein erfolgreiches Upgrade auf eine neue Version der HMC-Software durchgeführt wurde.

Anmerkung: Um Daten auf einem austauschbaren Datenträger sichern zu können, muss dieser verfügbar sein.

Führen Sie die folgenden Schritte aus, um HMC-Daten zu sichern:

Vorgehensweise

1. Wenn Sie auf einem Datenträger sichern wollen, führen Sie die folgenden Schritte zur Formatierung des Datenträgers aus:
   a. Legen Sie den Datenträger in das Laufwerk ein.
   b. Klicken Sie im Navigationsbereich auf das Symbol **Wartungsfähigkeit**  und wählen Sie anschließend **Service-Management** aus.
   c. Klicken Sie im Inhaltsbereich auf **Datenträger formatieren**.
   d. Wählen Sie den Datenträgertyp aus.
   e. Wählen Sie den Formattyp aus.
   f. Klicken Sie auf **OK**.
2. Klicken Sie im Navigationsbereich auf das Symbol **HMC-Verwaltung**  und wählen Sie anschließend **Konsolenverwaltung** aus.
3. Klicken Sie im Inhaltsbereich auf **Daten der Managementkonsole sichern**.
   Das Fenster **Daten der Managementkonsole sichern** wird geöffnet.
4. Wählen Sie eine Archivierungsoption aus.
   Sie können Daten auf einem lokalen System auf Datenträgern oder auf einem fernen System, das an das HMC-Dateisystem angehängt ist (zum Beispiel NFS), sichern. Sie können die gesicherten Daten aber auch über FTP an einen fernen Standort senden.
   - Zum Sichern auf einem lokalen System wählen Sie **Auf Datenträger eines lokalen Systems sichern** aus und befolgen Sie die Anweisungen.

- Zum Sichern auf einem angehängten fernen System wählen Sie **Auf angehängtem fernen System sichern** aus und befolgen Sie die Anweisungen.
- Zum Sichern auf einer fernen FTP-Site wählen Sie **Gesicherte kritische Daten an fernen Standort senden** aus und befolgen Sie die Anweisungen.

5. Fahren Sie mit „Schritt 5. Aktuelle HMC-Konfigurationsdaten notieren” auf Seite 87 fort.

Schritt 5. Aktuelle HMC-Konfigurationsdaten notieren

Informationen zu diesem Vorgang

Bevor Sie ein Upgrade auf eine neue Version der HMC-Software durchführen, sollten Sie die HMC-Konfigurationsdaten vorsichtshalber notieren.

Führen Sie die folgenden Schritte aus, um die aktuelle HMC-Konfiguration zu notieren:

Vorgehensweise

1. Wählen Sie ein verwaltetes System oder die Partitionen aus, für das bzw. die Sie HMC-Konfigurationsdaten aufzeichnen wollen.
2. Wählen Sie im Menü-Pod **Aktionen** > **Operationen planen** aus.

   Alle geplanten Operationen für das ausgewählte Ziel werden angezeigt.
3. Wählen Sie **Sortieren** > **Nach Objekt** aus.
4. Wählen Sie die einzelnen Objekte aus und notieren Sie die folgenden Details:
   - Objektname
   - Plandatum
   - Uhrzeit der Operation (wird im 24-Stunden-Format angezeigt)
   - Wiederkehrend (wenn Ja, führen Sie die folgenden Schritte aus):
     a. Wählen Sie **Anzeigen** > **Details zur Planung** aus.
     b. Notieren Sie die Intervallinformationen.
     c. Schließen Sie das Fenster "Geplante Vorgänge".
     d. Wiederholen Sie diese Schritte für jeden geplanten Vorgang.
5. Schließen Sie das Fenster **Geplante Operationen anpassen**.
6. Fahren Sie mit „Schritt 6. Status des fernen Befehls notieren” auf Seite 87 fort.

Schritt 6. Status des fernen Befehls notieren

Informationen zu diesem Vorgang

Führen Sie die folgenden Schritte aus, um den Status des fernen Befehls zu notieren:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf das Symbol **Benutzer und Sicherheit**  und wählen Sie anschließend **System- und Konsolensicherheit** aus.
2. Klicken Sie im Inhaltsbereich auf **Ausführung von fernen Befehlen aktivieren**.
3. Notieren Sie, ob das Markierungsfeld **Ausführung von fernen Befehlen über den ssh-Befehl** ausgewählt ist.
4. Klicken Sie auf **Abbrechen**.
5. Fahren Sie mit „Schritt 7. Upgradedaten speichern” auf Seite 88 fort.

Schritt 7. Upgradedaten speichern

Informationen zu diesem Vorgang

Sie können die aktuelle HMC-Konfiguration in einer designierten Plattenpartition auf der HMC oder auf einem lokalen Datenträger speichern. Speichern Sie Upgradedaten lediglich unmittelbar vor dem Upgrade der HMC-Software auf ein neues Release. Sie können die HMC-Konfigurationseinstellungen nach dem Upgrade wiederherstellen.

Anmerkung: Es ist nur eine Version der Sicherungsdaten zulässig. Bei jedem Speichern von Upgradedaten wird die vorherige Version überschrieben.

Führen Sie die folgenden Schritte aus, um Upgradedaten zu speichern:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf das Symbol **HMC-Verwaltung**  und wählen Sie anschließend **Konsolenverwaltung** aus.
2. Klicken Sie im Inhaltsbereich auf **Upgradedaten speichern**. Der Assistent **Upgradedaten speichern** wird geöffnet.
3. Wählen Sie den Datenträger aus, auf dem die Upgradedaten gespeichert werden sollen. Wenn Sie Daten auf einem austauschbaren Datenträger speichern möchten, legen Sie diesen jetzt ein. Klicken Sie auf **Weiter**.
4. Klicken Sie auf **Fertig stellen**.
5. Warten Sie, bis die Task beendet ist.

   Wenn die Operation zum Speichern von Upgradedaten fehlschlägt, wenden Sie sich an die nächste Unterstützungsstufe, bevor Sie fortfahren.

   Anmerkung: Setzen Sie den Upgradeprozess nicht fort, wenn die Operation zum Speichern von Upgradedaten fehlschlägt.
6. Klicken Sie auf **OK**.
7. Fahren Sie mit „Schritt 8. Upgrade der HMC-Software” auf Seite 88 fort.

Schritt 8. Upgrade der HMC-Software

Informationen zu diesem Vorgang

Zum Upgrade der HMC-Software starten Sie das System mit dem austauschbaren Datenträger im DVD-Laufwerk erneut.

Vorgehensweise

1. Legen Sie den Datenträger für die HMC-Produktinstallation in das DVD-Laufwerk ein.
2. Klicken Sie im Navigationsbereich auf das Symbol **HMC-Verwaltung**  und wählen Sie anschließend **Konsolenverwaltung** aus.
3. Wählen Sie im Inhaltsbereich **Managementkonsole herunterfahren oder erneut starten**.
4. Vergewissern Sie sich, ob **HMC erneut starten** ausgewählt wurde.
5. Klicken Sie auf **OK**.

   Die HMC wird erneut gestartet und die Systeminformationen werden im Fenster nacheinander angezeigt.
6. Wählen Sie **Upgrade** und klicken Sie auf **Weiter**.
7. Wählen Sie eine der folgenden Optionen aus:

- Wenn Sie die Upgradedaten bei der vorhergehenden Task gespeichert haben, fahren Sie mit dem nächsten Schritt fort.
- Wenn Sie die Upgradedaten in dieser Prozedur noch nicht gespeichert haben, müssen Sie die Upgradedaten jetzt speichern, bevor Sie die Arbeit fortsetzen.

8. Wählen Sie **Upgrade von Datenträger** aus und klicken Sie auf **Weiter**.
9. Bestätigen Sie die Einstellungen und klicken Sie auf **Fertig stellen**.
10. Folgen Sie den Bedienerführungen.

    Anmerkung:

    - Wenn die Anzeige leer ist, drücken Sie die Leertaste, um die Informationen anzuzeigen.
    - Die Installation der ersten DVD kann ca. 20 Minuten dauern.

11. Melden Sie sich im Anmeldedialog mit Ihrer Benutzer-ID und Ihrem Kennwort an.

    Die Installation des HMC-Codes ist beendet.
12. Fahren Sie mit „Schritt 9. Überprüfen, ob das Upgrade für den HMC-Maschinencode erfolgreich installiert wurde" auf Seite 89 fort.

Schritt 9. Überprüfen, ob das Upgrade für den HMC-Maschinencode erfolgreich installiert wurde

Informationen zu diesem Vorgang
Führen Sie die folgenden Schritte aus, um zu überprüfen, ob das HMC-Upgrade erfolgreich installiert wurde:

Vorgehensweise

1. Klicken Sie im Navigationsbereich auf das Symbol **HMC-Verwaltung**  und wählen Sie anschließend **Konsolenverwaltung** aus.
2. Klicken Sie im Inhaltsbereich auf **Hardware Management Console aktualisieren**.
3. Sehen Sie sich im neuen Fenster die Informationen an, die unter der Überschrift zu aktuellen HMC-Treiberinformationen angezeigt werden (einschließlich HMC-Version, Release, Programmfix, Erstellungsstufe und Basisversion), und notieren Sie die Informationen.
4. Überprüfen Sie, ob die Version und das Release dem installierten Update entsprechen.
5. Wenn die angezeigte Codeversion nicht mit der installierten Version übereinstimmt, führen Sie die Upgrade-Task mit einer neuen DVD erneut aus. Wenn das Problem bestehen bleibt, wenden Sie sich an die nächste Unterstützungsstufe.

HMC von fernem Standort aus mit Netzaktualisierungsimages aktualisieren

Dieser Abschnitt enthält Informationen darüber, wie ein Upgrade der Software auf einer HMC von einem fernen Standort aus mithilfe von Netzaktualisierungsimages aktualisiert wird.

Informationen zu diesem Vorgang
Dieser Abschnitt enthält Informationen darüber, wie ein Upgrade der Software auf einer HMC von einem fernen Standort aus mithilfe von Netzaktualisierungsimages aktualisiert wird.

Vorgehensweise

1. Rufen Sie von einem Computer oder Server mit Internetverbindung die Website Hardware Management Console Support and downloads (http://www14.software.ibm.com/webapp/set2/sas/f/hmcl/home.html) auf.

2. Laden Sie die entsprechenden Netzimages für HMC V9 herunter und speichern Sie diese auf einem FTP-Server.

   Ein direkter Download dieser Dateien auf die HMC ist nicht möglich. Stattdessen müssen die Imagedateien auf einen Server heruntergeladen werden, der FTP-Anforderungen akzeptiert.
3. Stellen Sie sicher, dass folgende Dateien heruntergeladen werden:
   - img2a
   - img3a
   - base.img
   - disk1.img
   - hmcnetworkfiles.sum
4. Speichern Sie die Upgradedaten auf der HMC. Führen Sie zum Speichern der Upgradedaten die folgenden Befehle aus:
   - Führen Sie folgende Befehle aus, um die Daten sowohl auf DVD als auch auf der Festplatte zu speichern:

     mount /media/cdrom

     saveupgdata -r diskdvd
   - Führen Sie folgende Befehle aus, um die Daten auf der Festplatte zu speichern:

     saveupgdata -r disk
5. Kopieren Sie die Upgrade-Dateien auf die bootfähige Plattenpartition auf der HMC. Führen Sie den Befehl **getupgfiles** aus, um die Dateien zu kopieren.

   Beispiel: **getupgfiles -h <FTP-Server> -u <Benutze-ID> -d <fernes Verzeichnis>**

   Dabei gilt Folgendes:
   - **FTP-Server** ist der Hostname oder die IP-Adresse des FTP-Servers, auf den die HMC-Netzimages heruntergeladen wurden.
   - **Benutzer-ID** ist eine gültige Benutzer-ID für den FTP-Server. Wenn Sie im obigen Befehl kein Kennwort mithilfe des Arguments `--passwd` angeben, werden Sie zur Eingabe des Kennworts aufgefordert.
   - **Fernes_Verzeichnis** ist das Verzeichnis auf dem FTP-Server, in dem die HMC-Netzimages gespeichert sind.
6. Starten Sie die HMC neu, um den Code, der in die bootfähige Partition kopiert wurde, zu aktualisieren. Führen Sie für den Neustart der HMC den Befehl **chhmc -c altdiskboot -s enable --mode upgrade** aus.
7. Starten Sie die HMC neu und starten Sie das Upgrade. Führen Sie zum Starten des Upgrades den Befehl **hmcshutdown -r -t now** aus.

HMC sichern

Dieser Abschnitt enthält Informationen darüber, wie Sie die Sicherheit Ihrer Hardware Management Console (HMC) erhöhen, die auf Ihren Unternehmenssicherheitsstandards basiert.

Die Standardkonfiguration der HMC bietet für die meisten Unternehmensbenutzer reichlich Sicherheit. Mit der Hardware Management Console (HMC) ab Version 8.4.0 können Sie die Sicherheit der HMC, die auf Ihren Unternehmenssicherheitsstandards basiert, weiter erhöhen. Zur Erhöhung der Sicherheit der HMC müssen Sie für die HMC mindestens die Sicherheitsstufe 1 festlegen. Abhängig von Ihrer Umgebung und den Anforderungen an die Unternehmenssicherheit können Sie auch Stufe 2 oder Stufe 3 auswählen.

Anmerkung: Halten Sie vor einer Änderung der Sicherheitsstufe Rücksprache mit Ihrem Compliance-Team für Unternehmenssicherheit.

Sicherheitsstufe 1

Führen Sie die folgenden Schritte aus, um die HMC zu sichern (Sicherheitsstufe 1):

1. Ändern Sie das vordefinierte Kennwort des Standardbenutzers `hscroot`. Weitere Informationen zur Kennwortrichtlinie finden Sie unter „Erweiterte Kennwortrichtlinie” auf Seite 92.
2. Wenn die HMC nicht Teil einer physisch sicheren Umgebung ist, legen Sie das Kennwort `grub` fest, indem Sie folgenden Befehl ausführen: `chhmc -c grubpasswd -s enable --passwd <neues Grub-Kennwort>`
3. Wenn Sie das integrierte Managementmodul (IMM) auf der HMC konfiguriert haben, legen Sie ein sicheres IMM-Kennwort fest.
4. Legen Sie für den Benutzer *admin* und Endbenutzer auf allen Servern ein sicheres Kennwort fest.
5. Aktualisieren Sie die HMC mit den neuesten freigegebenen Sicherheitsfixes. Weitere Informationen zu den Sicherheitsfixes finden Sie unter IBM Fix Central.

Sicherheitsstufe 2

Führen Sie die folgenden Schritte zur Erhöhung der Sicherheit für die HMC aus, wenn Sie über mehrere Benutzer verfügen:

1. Erstellen Sie für jeden Benutzer auf der HMC ein Konto und weisen Sie den Benutzern die erforderlichen Rollen und Ressourcen zu. Weitere Informationen zu den verschiedenen Rollen auf der HMC finden Sie unter HMC-Tasks, Benutzerrollen, IDs und zugehörige Befehle.

   Anmerkung: Stellen Sie sicher, dass Sie nur die erforderlichen Rollen und Ressourcen für Benutzer zuweisen, die auf der HMC erstellt wurden. Sie können bei Bedarf auch benutzerdefinierte Rollen erstellen.
2. Aktivieren Sie die Benutzerdatenreplikation zwischen verschiedenen Hardware Management Consoles. Die Benutzerdatenreplikation kann im Modus \"Master-Slave\" oder im Modus \"Peer-Peer\" durchgeführt werden. Weitere Informationen zur Benutzerdatenreplikation finden Sie unter Datenreplikation verwalten.
3. Importieren Sie ein Zertifikat, das von der Zertifizierungsstelle signiert wurde.

Sicherheitsstufe 3

Führen Sie die folgenden Schritte zur Erhöhung der Sicherheit für die HMC aus, wenn Sie über mehrere Hardware Management Consoles und Systemadministratoren verfügen:

1. Verwenden Sie eine zentrale Authentifizierung, wie z. B. das Lightweight Directory Access Protocol (LDAP) oder Kerberos. Weitere Informationen zum Konfigurieren des LDAP finden Sie unter LDAP auf der HMC konfigurieren.
2. Aktivieren Sie die Benutzerdatenreplikation zwischen verschiedenen Hardware Management Consoles.
3. Stellen Sie sicher, dass sich die HMC im Modus NIST SP 800-131A befindet, damit sie nur sichere Verschlüsselungen verwendet.
4. Blockieren Sie Anschlüsse, die in der Firewall nicht erforderlich sind. Weitere Informationen zu den verwendbaren HMC-Anschlüssen finden Sie in der folgenden Tabelle:

Tabelle 32. Vom Benutzer verwendeter Anschluss für die Interaktion mit der HMC

Anschluss	Beschreibung	Typ	Protokollversion (Standardmodus)	Protokollversion (NIST-Modus)
22	Open SSH	TCP	SSH v3	SSH v3
123	NTP	UDP	NTP	NTP
161	SNMP-Agent	UDP	SNMP v3	SNMP v3

Tabelle 32. Vom Benutzer verwendeter Anschluss für die Interaktion mit der HMC (Forts.)

Anschluss	Beschreibung	Typ	Protokollversion (Standardmodus)	Protokollversion (NIST-Modus)
162	SNMP-Trap	UDP	SNMP v3	SNMP v3
427	SLP	UDP	N/V	N/V
443	HMC-GUI und REST-API	TCP	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)
657	RMC	TCP/UDP	RSCT (Klartext + Hash-and-Sign)	RSCT (Klartext + Hash-and-Sign)
2300	5250-Terminal für IBM i	TCP	Klartext	Klartext
2301	Sicheres 5250-Terminal für IBM i	TCP	TLS 1.2	TLS 1.2
5989	CIM (Legacy-Anschluss, nicht funktionsfähig)	TCP	Nicht funktionsfähig	Nicht funktionsfähig
9900	FCS: HMC-HMC-Erkennung	UDP	FCS	FCS
9920	FCS: HMC-HMC-Kommunikation	TCP	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)
9960	VTerm-Applet in GUI	TCP	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)
12443	HMC-REST-API (Legacy-Anschluss)	TCP	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)
12347	RSCT-Peerdomäne	UDP	RSCT (Klartext + Hash-and-Sign)	RSCT (Klartext + Hash-and-Sign)
12348	RSCT-Peerdomäne	UDP	RSCT (Klartext + Hash-and-Sign)	RSCT (Klartext + Hash-and-Sign)

Notes:

- Sie dürfen nur SSH (Anschluss 22), HTTPS (Anschluss 443 und 12443), das sichere 5250-Terminal für IBM i (Anschluss 2301) und VTerm (Anschluss 9960) verwenden, die in einem Intranet zugänglich gemacht wurden. Alle anderen Anschlüsse müssen in einem privaten bzw. isolierten Netz verwendet werden. Für das Resource Monitoring and Control (RMC) (Anschluss 657), FCS (Anschluss 9900 und Anschluss 9920) und die RSCT-Peerdomäne (Anschluss 12347 und Anschluss 12348) können Sie einen separaten Ethernet-Anschluss und separates VLAN verwenden.
- Unter dem Befehl **`netstat`** aufgeführte Anschlüsse werden nur für interne Prozesse verwendet.

Erweiterte Kennwortrichtlinie

Sie können mit der Hardware Management Console (HMC) Kennwortanforderungen für lokal authentifizierte Benutzer durchsetzen. Mit der Funktion für die erweiterte Kennwortrichtlinie kann der Systemadministrator Kennworteinschränkungen festlegen. Die erweiterte Kennwortrichtlinie gilt für die Systeme, auf denen eine HMC installiert ist.

Systemadministratoren können die erweiterte Kennwortrichtlinie verwenden, um für alle Benutzer eine einzige Kennwortrichtlinie zu definieren. Die HMC stellt eine Kennwortrichtlinie für mittlere Sicherheit bereit, die von den Systemadministratoren zum Festlegen von Kennworteinschränkungen aktiviert werden kann. Der Systemadministrator kann zudem entscheiden, ob die Richtlinie für mittlere Sicherheit oder eine neue, benutzerdefinierte Richtlinie aktiviert werden soll. Die Kennwortrichtlinie der HMC für mittlere Sicherheit kann nicht von dem System entfernt werden. In der folgenden Tabelle werden die Attribute der Richtlinie für mittlere Sicherheit und die Standardwerte aufgelistet.

Tabelle 33. Kennwortattribute für die Kennwortrichtlinie der HMC für mittlere Sicherheit

Attribut	**Beschreibung**	**Standardwert**
`min_pwage`	Die Mindestanzahl von Tagen, die ein Kennwort aktiv bleiben muss.	1
`pwage`	Die maximale Anzahl von Tagen, die ein Kennwort aktiv bleiben könnte.	180
`min_length`	Die Mindestlänge eines Kennworts.	8
`hist_size`	Die Anzahl der zuvor gespeicherten Kennwörter, die nicht wiederverwendet werden können.	10
`warn_pwage`	Bei nahendem Ablauf des Kennworts die Anzahl der Tage, bis ein Benutzer eine entsprechende Warnung erhält.	7
`min_digits`	Die Mindestanzahl der im Kennwort zu verwendenden Ziffern.	Keiner
`min_uppercase`	Die Mindestanzahl der Großbuchstaben.	1
`min_lowercase`	Die Mindestanzahl der Kleinbuchstaben.	6
`min_special_chars`	Die Mindestanzahl der im Kennwort zu verwendenden Sonderzeichen.	Keiner

Beachten Sie bei der Kennwortrichtlinie der HMC für mittlere Sicherheit die folgenden Punkte:

- Die Richtlinie gilt nicht für die Benutzer-IDs **hscroot**, **hscpe** und **root**.
- Die Richtlinie wirkt sich nur auf die lokal authentifizierten Benutzer aus, die von der HMC verwaltet werden, und kann für LDAP- oder Kerberos-Benutzer nicht durchgesetzt werden.
- Mit der Kennwortrichtlinie der HMC für mittlere Sicherheit bzw. der benutzerdefinierten Richtlinie können die Systemadministratoren Einschränkungen für die Wiederverwendung von Kennwörtern festlegen.
- Das Kennwort der HMC für mittlere Sicherheit ist schreibgeschützt und die Attribute des Kennworts der HMC für mittlere Sicherheit können nicht geändert werden. Sie können ein neues, benutzerdefiniertes Kennwort erstellen, um Kennworteinschränkungen festzulegen.

Sie können folgende Befehle verwenden, um die Kennwortrichtlinie der HMC für mittlere Sicherheit zu konfigurieren:

mkpwdpolicy
: Importiert die Kennwortrichtlinie aus einer Datei, die alle Parameter enthält, oder erstellt eine Kennwortrichtlinie.

lspwdpolicy
: Listet alle verfügbaren Kennwortrichtlinienprofile auf und sucht nach bestimmten Parametern. Sie können auch die Kennwortrichtlinie anzeigen, die derzeit aktiv ist.

rmpwdpolicy
: Entfernt eine vorhandene inaktive Kennwortrichtlinie.

Anmerkung: Es ist nicht möglich, eine aktive Richtlinie für mittlere Sicherheit und die schreibgeschützte Standardkennwortrichtlinie zu entfernen.

chpwdpolicy
Ändert Parameter einer inaktiven Kennwortrichtlinie.

Sicherheitsprofile: Datenschutzgrundverordnung (DSGVO) und Payment Card Industry Data Security Standard (PCI-DSS)

Dieser Abschnitt enthält Informationen darüber, wie die Hardware Management Console (HMC) die Datenschutzinformationen der Benutzer verarbeitet.

Bei der Hardware Management Console (HMC) handelt es sich um eine geschlossene Appliance, die keine Karteninhaberdaten speichert. Daher findet nur eine Teilmenge der im PCI-DSS definierten Anforderungen und Sicherheitsbewertungsverfahren der IT-Sicherheit Anwendung auf die HMC. Auf der HMC kann nur vertrauenswürdiger, von IBM verteilter Code installiert werden. Bei Bekanntwerden von Sicherheitslücken durch den IBM PSIRT-Prozess (PSIRT = Product Security Incident Response Team, für Sicherheitsverstöße zuständiges IBM Team) werden vorläufige Fixes veröffentlicht. Die Anforderungen und Empfehlungen umfassen folgende Punkte:

Fragen zur DSGVO

Tabelle 34. Fragen zur DSGVO . Die Tabelle enthält Informationen zu den Fragen zur DSGVO.

Fragen	**Antworten**
Welche Art von Daten wird in der HMC gespeichert?	Die HMC speichert Konfigurationsdaten von Power-Hardware, der PowerVM-Virtualisierung und Informationen zu den Leistungsmetriken.
Verarbeitet die HMC personenbezogene Daten?	Sie können Kontaktinformationen für die Call-Home-Funktion bereitstellen. Die Bereitstellung von Kontaktinformationen für die Call-Home-Funktion ist optional.
Welche vordefinierten Konten werden für die Systemverwaltung der HMC verwendet?	Der Systemadministrator verwendet den Benutzernamen *hscroot*.
Beziehen sich Konten in der HMC auf eine bestimmte Person?	Nein.
Müssen in der HMC personenbezogene Daten bereitgestellt werden?	Nein. Sie müssen keine personenbezogenen Daten bereitstellen. Die Bereitstellung dieser Daten ist optional.
Enthält die HMC-Protokolldatei personenbezogene Daten?	Nein.
Ist es möglich, personenbezogene Daten vollständig und endgültig zu löschen?	Ja. Hierzu muss die Call-Home-Funktion dekonfiguriert werden.

Fragen zum PCI-DSS

Tabelle 35. Fragen zum PCI-DSS . Die Tabelle enthält Informationen zu den Fragen zum PCI-DSS.

Fragen	Antworten
Wie kann eine Firewallkonfiguration zum Schutz der Karteninhaberdaten installiert und verwaltet werden?	Die HMC speichert keine Karteninhaberdaten und greift nicht darauf zu. Trotzdem verfügt die HMC über eine Firewallkonfiguration, die dem Benutzer die Kontrolle und Aktivierung bestimmter Anschlüsse ermöglicht.
Kann ich für Systemkennwörter und andere Sicherheitsparameter Werte der werkseitigen Voreinstellung verwenden?	Vor der Installation eines Systems im Netz sollten Sie sämtliche vordefinierten Kennwörter des Benutzers *hscroot* ändern.
Wie schützt die HMC die gespeicherten Karteninhaberdaten?	Die HMC speichert keine Karteninhaberdaten und greift nicht darauf zu.
Wie verschlüsselt die HMC die Karteninhaberdaten, wenn die Daten über offene öffentliche Netze übertragen werden?	Die HMC speichert keine Karteninhaberdaten und greift nicht darauf zu.
Wie können Programme mit Antivirensoftware verwendet und regelmäßig aktualisiert werden?	Bei der HMC handelt es sich um eine geschlossene Appliance. Daher kann sie nicht durch Malware infiziert werden.
Wie können sichere Systeme und Anwendungen entwickelt und verwaltet werden?	Sie müssen die erforderlichen Patches manuell über die Website IBM Fix Central auf Ihrem System installieren. Auf der HMC kann nur vertrauenswürdiger, von IBM verteilter Code installiert werden.
Wird der Zugriff auf die Karteninhaberdaten durch die HMC beschränkt?	Die HMC speichert keine Karteninhaberdaten und greift nicht darauf zu.
Wie kann den einzelnen Personen, die Zugriff auf den Computer haben, eine eindeutige ID zugewiesen werden?	Sie können diese Anforderung umsetzen, indem Sie sicherstellen, dass es keine gemeinsam genutzten IDs gibt, und indem Sie die Kennwortrichtlinien befolgen.
Wie kann der physische Zugriff auf die Karteninhaberdaten beschränkt werden?	Die HMC speichert keine Karteninhaberdaten und greift nicht darauf zu.
Wie kann der Zugriff auf Netzressourcen und die Karteninhaberdaten verfolgt und überwacht werden?	Die HMC speichert keine Karteninhaberdaten und greift nicht darauf zu.
Wie testet die HMC die Sicherheit von System und Prozessen?	Mithilfe von Überprüfungstools werden in allen freigegebenen Versionen der HMC Sicherheitsscans durchgeführt. Zu den Überprüfungstools zählen: *Qualys*, *Nessus*, *testssl*, *sslscan* und *ASoC*.
Wie kann eine Sicherheitsrichtlinie eingehalten werden, welche die Informationssicherheit für Mitarbeiter und Auftragnehmer beinhaltet?	Der Systemadministrator inaktiviert die Anmeldung ferner Benutzer, aktiviert die Benutzeranmeldung auf Grundlage des Bedarfs und inaktiviert die Benutzeranmeldung, wenn der Zugriff nicht mehr erforderlich ist.

Allgemeine Probleme beim Sichern der HMC beheben

In diesem Abschnitt erhalten Sie Informationen darüber, wie Sie einige Probleme beheben können, die ggf. beim Sichern der HMC auftreten.

Wie wird die Verbindung zwischen der Hardware Management Console (HMC) und dem System gesichert?

Die HMC ist über den flexiblen Serviceprozessor ((FSP) mit dem System verbunden. Für die Verwaltung der FSP- und Power-Hypervisoren wird ein proprietäres binäres Protokoll namens Network Client Protocol (NETC) verwendet. In der folgenden Tabelle werden die Anschlüsse aufgelistet, die von der HMC verwendet werden:

Tabelle 36. Anschlüsse am FSP für die Interaktion mit der HMC

Anschluss am FSP	Beschreibung	Protokollversion (Standardmodus)	Protokollversion (NIST-Modus)
443	Advanced System Management Interface	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)
30000	NETC	NETC (TLS 1.2). Greift für die Unterstützung älterer Firmware auf SSLv3 zurück.	NETC (TLS 1.2)
30001	VTerm	NETC (TLS 1.2). Greift für die Unterstützung älterer Firmware auf SSLv3 zurück.	NETC (TLS 1.2)

Wie kann die HMC gesperrt werden?

Wenn Sie die Sicherheit für Ihre Infrastruktur verbessern möchten, können Sie ein IPS-Gerät (IPS = Intrusion-Prevention-System) verwenden oder alle Hardware Management Consoles und IBM Power Systems-Server hinter einer Firewall hinzufügen. Darüber hinaus können Sie Netzservices auf der HMC inaktivieren, wenn Sie die HMC nicht über Fernzugriff verwenden oder Sie die HMC sperren möchten. Führen Sie die folgenden Schritte aus, um Netzservices auf der HMC zu inaktivieren:

1. Inaktivieren Sie die Ausführung von fernen Befehlen über den SSH-Anschluss.
2. Inaktivieren Sie das ferne virtuelle Terminal (VTerm-Anschluss).
3. Inaktivieren Sie den Webfernzugriff (HMC-GUI und REST-API).
4. Blockieren Sie Anschlüsse in der Firewall mithilfe der HMC-Netzeinstellungen für die einzelnen konfigurierten Ethernet-Anschlüsse.

Wie kann die HMC in den Konformitätsmodus "NIST SP 800-131A" versetzt werden?

Bei Verwendung der HMC ab Version 8.1.0 werden nur sichere Verschlüsselungen unterstützt, die unter NIST SP 800-131A aufgeführt werden. Sie können ggf. keine Verbindung zu älteren Power Systems-Servern herstellen, z. B. zu POWER5-Servern, die Transport Layer Security (TLS 1.2) nicht unterstützen. Weitere Informationen zum Ändern des Sicherheitsmodus finden Sie unter NIST-Modus der HMC Version 8, Release 8.

Wie können von der HMC verwendete Verschlüsselungen angezeigt und geändert werden?

Bei Verwendung der HMC ab Version 8.1.0 unterstützt die HMC sicherere Verschlüsselungssätze, die in NIST 800-131A definiert sind. Im Standardmodus verwendete Verschlüsselungen sind sicher. Führen Sie den Befehl **`lshmcencr`** aus, um weitere Informationen zu von der HMC unterstützten Verschlüsselungswerten zu erhalten. Wenn Ihre Unternehmensstandards die Verwendung eines anderen Verschlüsselungssatzes erforderlich machen, führen Sie den Befehl **`chhmcencr`** aus, um die Verschlüsselungssätze zu ändern.

Führen Sie den folgenden Befehl aus, um die Verschlüsselungswerte aufzulisten, die von der HMC zum Verschlüsseln des Benutzerkennworts verwendet werden:

```
lshmcencr -c passwd -t c
```

Führen Sie den folgenden Befehl aus, um die Verschlüsselungswerte aufzulisten, die derzeit von der Webbenutzerschnittstelle der HMC und der REST-API verwendet werden:

```
lshmcencr -c webui -t c
```

Führen Sie den folgenden Befehl aus, um die Verschlüsselungswerte und den MAC-Algorithmus aufzulisten, die derzeit von der SSH-Schnittstelle der HMC verwendet werden können:

```
lshmcencr -c ssh -t c
```

```
lshmcencr -c sshmac -t c
```

Wie kann die Sicherheit des Zertifikats auf der HMC geprüft werden?

Die selbst signierten Zertifikate auf der HMC verwenden SHA256 mit RSA-Verschlüsselung mit einem 2048-Bit-Schlüssel. Dieses Verschlüsselungsverfahren ist sicher. Wenn Sie CA-signierte Zertifikate verwenden, sollten Sie sicherstellen, dass Sie keine Verschlüsselung mit 1024-Bit-Schlüssel verwenden. Dieses Verschlüsselungsverfahren ist unsicher. Für die HMC können folgende Zertifikate verwendet werden:

- Das CA-signierte Zertifikat kann für die HMC-GUI und die REST-API verwendet werden (Anschlüsse 443 und 12443).
- Der Anschluss 9920 wird für die Kommunikation zwischen HMCs verwendet. Sie können dieses Zertifikat nicht durch Ihr eigenes Zertifikat ersetzen.

Wie wählt man sich zwischen einem selbst signierten Zertifikat (Standard) und einem CA-signierten Zertifikat aus?

Die HMC generiert während der Installation automatisch ein Zertifikat. Sie können jedoch auch über die HMC eine Zertifikatssignieranforderung (Certificate Signing Request, CSR) generieren und ein neues Zertifikat abrufen, das von einer Zertifizierungsstelle ausgestellt wurde. Sie können dieses Zertifikat in die HMC importieren. Stellen Sie sicher, dass Sie auch einen Domänennamen für die HMC abrufen. Weitere Einzelheiten zur Verwaltung der Zertifikate auf der HMC finden Sie unter Zertifikate verwalten.

Wie kann auf der HMC ein Audit durchgeführt werden?

Der Schwerpunkt des Audits auf der Hardware Management Consoles liegt auf konfigurierten Verschlüsselungen und der Nutzungsaktivität der verschiedenen HMC-Benutzer. Verwenden Sie die folgenden Befehle, um die Nutzungsaktivität verschiedener HMC-Benutzer anzuzeigen:

Tabelle 37. Von der HMC verwendete Verschlüsselungen

Verwendungszweck	**Befehl**
Kennwortverschlüsselung (globale Einstellung)	`lshmcencr -c passwd -t c`
Kennwortverschlüsselung für die einzelnen Benutzer	`lshmcusr -Fname:password_encryption`
SSH-Verschlüsselungen	`lshmcencr -c ssh -t c`
SSH-MAC	`lshmcencr -c sshmac -t c`
Für die HMC-GUI und REST-API verwendete Verschlüsselungen	`lshmcencr -c webui -t c`

Verwenden Sie die folgenden Befehle, um verschiedene Informationen zu Konsolen und wartungsfähigen Ereignissen für die Verwendung in der HMC zu überwachen:

Tabelle 38. Befehle zum Anzeigen der angemeldeten Benutzer sowie von Informationen zu Konsolen oder wartungsfähigen Ereignissen in der HMC

Informationen	**Befehl**
GUI-Benutzer	`lslogon –r webui –u`
GUI-Tasks	`lslogon –r webui –t`
CLI-Benutzer	`lslogon –r ssh –u`
CLI-Tasks	`lslogon –r ssh –t`
Vorgänge auf der HMC	`lssvcevents -t console -d <Anzahl von Tagen>`
Vorgänge auf dem System	`lssvcevents –t hardware –m <verwaltetes System> -d <Anzahl von Tagen>`

Zentrale Überwachungsereignisse für die HMC: Wenn Sie über viele Hardware Management Consoles verfügen, legen Sie fest, dass alle Nutzungsdaten in der `rsyslog`-Datei gesammelt werden.

Wie behebt IBM die HMC-Sicherheitslücken?

IBM verfügt über einen Prozess für die Reaktion auf Sicherheitsvorfälle namens IBM Product Security Incident Response Team (PSIRT). Bei dem für Sicherheitsverstöße zuständigen IBM Team (IBM Product Security Incident Response Team, PSIRT) handelt es sich um ein globales Team, das den Eingang, die Untersuchung und die interne Koordination von Informationen zu Sicherheitslücken in Bezug auf Angebote von IBM verwaltet. Open-Source-Komponenten und IBM Komponenten, die im Lieferumfang der HMC enthalten sind, werden aktiv überwacht und analysiert. IBM stellt vorläufige Fixes und Sicherheitsfixes für alle unterstützten Releases der HMC bereit.

Wie können neue vorläufige Fixes auf der HMC verfolgt werden?

Das Sicherheitsbulletin enthält Informationen zu den Sicherheitslücken und vorläufige Fixes für unterstützte HMC-Versionen. Wenn Sie vorläufige Fixes auf der HMC verfolgen möchten, haben Sie folgende Möglichkeiten:

- Suchen Sie auf der folgenden Website nach den neuesten Sicherheitsbulletins: IBM Security Bulletin.
- Folgen Sie @IBMPowereSupp auf Twitter, um Benachrichtigungen zu erhalten.
- Abonnieren Sie E-Mail-Benachrichtigungen unter IBM Support.

HMC-Anschlusspositionen

Sie können anhand von Positionscodes nach Anschlusspositionen suchen. Verwenden Sie die Abbildungen zu den HMC-Anschlusspositionen, um einen Positionscode der HMC-Anschlussposition auf dem Server zuzuordnen.

HMC-Anschlusspositionen - Modell 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H und 9223-22S

Verwenden Sie dieses Diagramm und diese Tabelle, um die HMC-Anschlüsse für 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H und 9223-22S zuzuordnen.

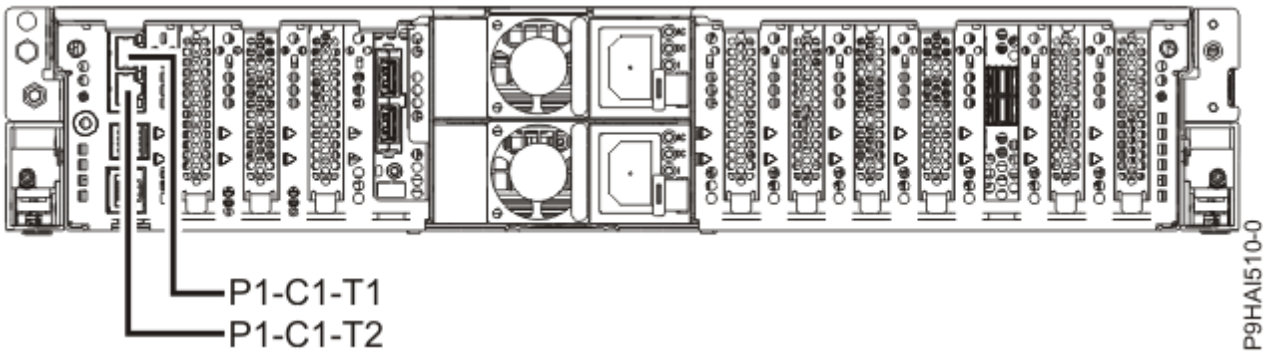


Abbildung 10. HMC-Anschlusspositionen - 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H und 9223-22S

Tabelle 39. HMC-Anschlusspositionen - 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H und 9223-22S		
Anschluss	**Code für physische Position**	**Kennzeichnungs-LED**
HMC-Anschluss 1	Un-P1-C1-T1	Nein
HMC-Anschluss 2	Un-P1-C1-T2	Nein
Weitere Informationen zu HMC-Anschlusspositionen für das System vom Typ 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H oder 9223-22S finden Sie unter Teileposition und Positionscodes für das System vom Typ 9008-22L, 9009-22A, 9009-22G, 9223-22H oder 9223-22S.		

HMC-Anschlusspositionen - Modell 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H und 9223-42S

Verwenden Sie dieses Diagramm und diese Tabelle, um die HMC-Anschlüsse für 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H und 9223-42S zuzuordnen.

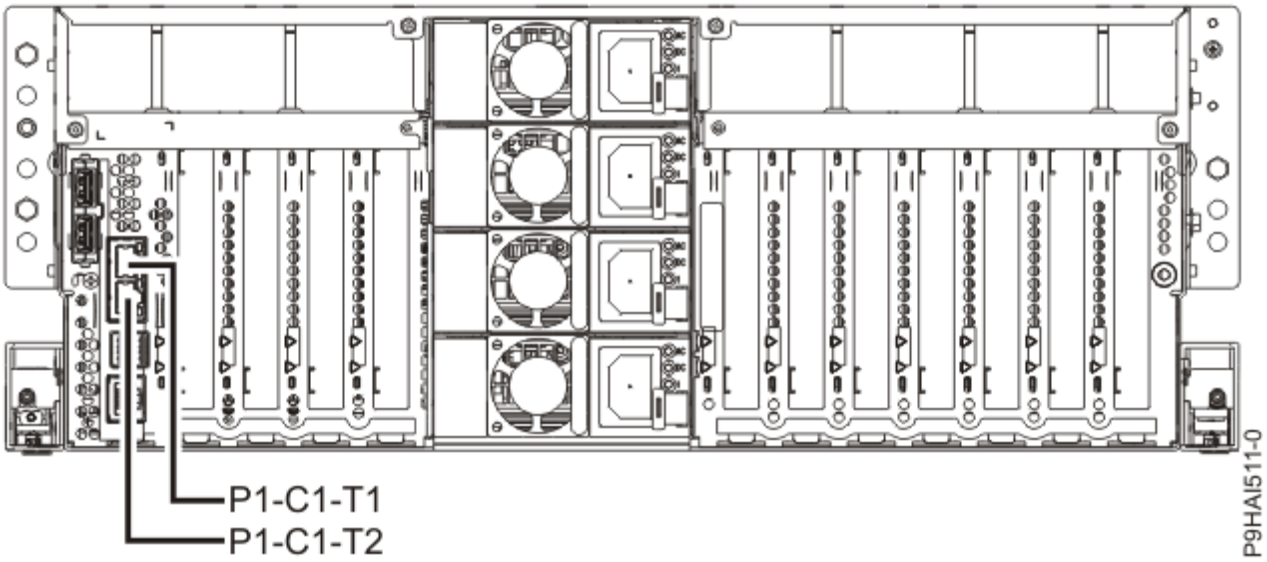


Abbildung 11. HMC-Anschlusspositionen - 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H und 9223-42S

Tabelle 40. HMC-Anschlusspositionen - 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H und 9223-42S		
Anschluss	**Code für physische Position**	**Kennzeichnungs-LED**
HMC-Anschluss 1	Un-P1-C1-T1	Nein
HMC-Anschluss 2	Un-P1-C1-T2	Nein
Weitere Informationen zu HMC-Anschlusspositionen für das System vom Typ 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H oder 9223-42S finden Sie unter Teileposition und Positionscodes für das System vom Typ 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H oder 9223-42S.		

HMC-Anschlusspositionen für Modell 9040-MR9

Verwenden Sie dieses Diagramm und diese Tabelle, um die HMC-Anschlüsse für 9040-MR9 zuzuordnen.

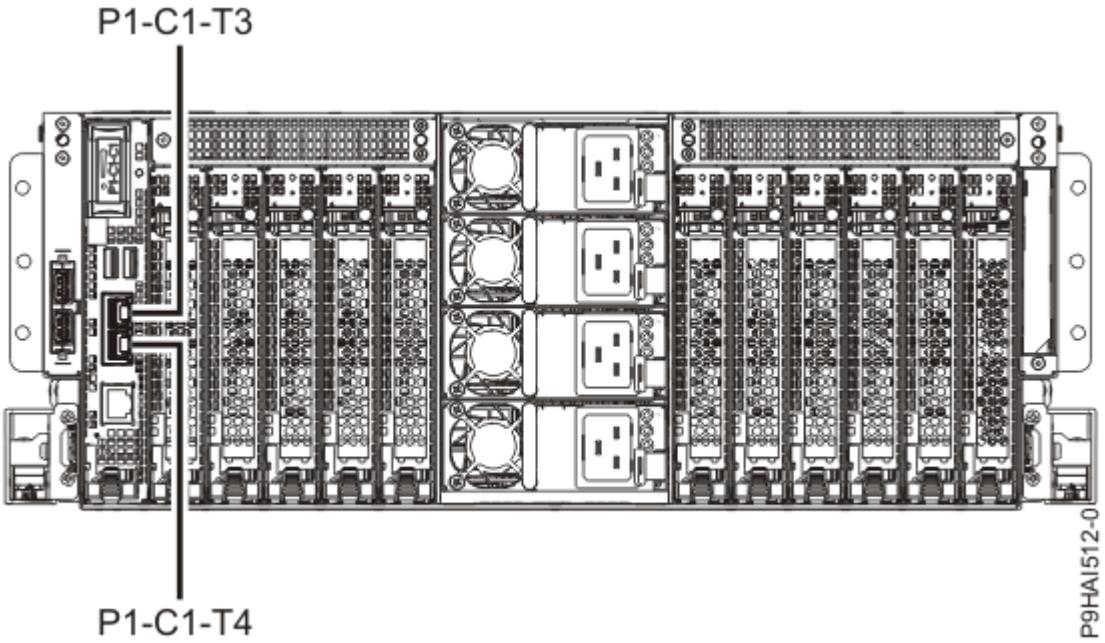


Abbildung 12. HMC-Anschlusspositionen für 9040-MR9

Tabelle 41. HMC-Anschlusspositionen für 9040-MR9		
Anschluss	**Code für physische Position**	**Kennzeichnungs-LED**
HMC-Anschluss 1	Un-P1-C1-T3	Nein
HMC-Anschluss 2	Un-P1-C1-T4	Nein
Weitere Informationen zu HMC-Anschlusspositionen für das System vom Typ 9040-MR9 finden Sie unter Teileposition und Positionscodes.		

HMC-Anschlusspositionen für Modell 9080-M9S

Verwenden Sie dieses Diagramm und diese Tabelle, um die HMC-Anschlüsse für 9080-M9S zuzuordnen.

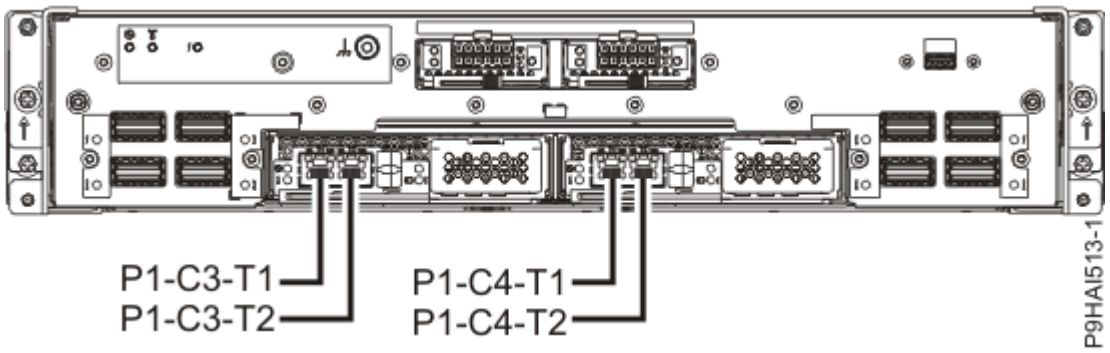


Abbildung 13. HMC-Anschlusspositionen für 9080-M9S

Tabelle 42. HMC-Anschlusspositionen für 9080-M9S		
Anschluss	**Position des physischen Anschlusses**	**Kennzeichnungs-LED**
Serviceprozessorkarte 1 - HMC-Anschluss 1	Un-P1-C3-T1	Nein
Serviceprozessorkarte 1 - HMC-Anschluss 2	Un-P1-C3-T2	Nein
Serviceprozessorkarte 2 - HMC-Anschluss 1	Un-P1-C4-T1	Nein
Serviceprozessorkarte 2 - HMC-Anschluss 2	Un-P1-C4-T2	Nein
Weitere Informationen zu HMC-Anschlusspositionen für das System vom Typ 9080-M9S finden Sie unter Teileposition und Positionscodes.		

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden.

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim zuständigen IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Services können auch andere, äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Produkten, Programmen und Services anderer Anbieter liegt beim Kunden.

Für die in diesem Handbuch beschriebenen Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Director of Licensing
IBM Europe, Middle East & Africa
Tour Descartes
2, avenue Gambetta
92066 Paris La Défense
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die hier enthaltenen Informationen werden in regelmäßigen Zeitabständen aktualisiert und als Neuausgabe veröffentlicht. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter werden lediglich als Service für den Kunden bereitgestellt und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Die genannten Leistungsdaten- und Kundenbeispiele dienen nur zur Veranschaulichung. Tatsächliche Leistungsergebnisse können, abhängig von bestimmten Konfigurationen und Betriebsbedingungen, variieren.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte, deren veröffentlichten Ankündigungen oder anderen allgemein verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Aussagen über Pläne und Absichten von IBM unterliegen Änderungen oder können zurückgenommen werden und repräsentieren nur die Ziele von IBM.

Alle von IBM angegebenen Preise sind empfohlene Richtpreise und können jederzeit ohne weitere Mitteilung geändert werden. Händlerpreise können u. U. von den hier genannten Preisen abweichen.

Diese Veröffentlichung dient nur zu Planungszwecken. Die in dieser Veröffentlichung enthaltenen Informationen können geändert werden, bevor die beschriebenen Produkte verfügbar sind.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufs. Sie sollen nur die Funktionen des Lizenzprogramms illustrieren und können Namen von Personen, Firmen, Marken oder Produkten enthalten. Alle diese Namen sind frei erfunden und jede Ähnlichkeit mit konkreten Personen oder Unternehmen ist rein zufällig.

Wird dieses Buch als Softcopy (Book) angezeigt, erscheinen keine Fotografien oder Farbabbildungen.

Diese Informationen wurden von IBM für die beschriebenen Maschinen erstellt. Für eine anderweitige Verwendung übernimmt IBM keine Verantwortung.

Die Datenverarbeitungssysteme von IBM sind so konzipiert, dass die Möglichkeit von nicht erkannten Datenbeschädigungen oder Dateiverlusten weitgehend eingeschränkt ist. Dieses Risiko kann jedoch nie ganz ausgeschlossen werden. Kunden, bei denen nicht geplante Systemausfälle oder Störungen, Netzstromschwankungen bzw. -ausfälle oder Komponentenfehler aufgetreten sind, müssen die zum Zeitpunkt der Ausfälle oder Störungen stattgefundenen Operationen und die dabei vom System gesicherten oder übertragenen Daten auf Vollständigkeit prüfen. Ferner müssen Kunden Verfahren etablieren, um sicherzustellen, dass eine unabhängige Datenprüfung durchgeführt wird, bevor Daten aus solchen sensiblen oder kritischen Operationen als zuverlässig angesehen werden. Kunden sollten die Websites von IBM regelmäßig auf aktualisierte Informationen und Fixes hin prüfen, die sich auf ihr System und die zugehörige Software beziehen.

Erklärung zur Homologation

Möglicherweise ist dieses Produkt in Ihrem Land nicht für den Anschluss an Schnittstellen von öffentlichen Telekommunikationsnetzen zertifiziert. Vor der Herstellung einer solchen Verbindung ist eine entsprechende Zertifizierung ggf. gesetzlich vorgeschrieben. Unterstützung erhalten Sie von einem IBM Ansprechpartner oder Reseller.

Funktionen zur barrierefreien Bedienung für IBM Power Systems-Server

Funktionen zur barrierefreien Bedienung unterstützen Benutzer mit einer Behinderung, wie z. B. einer eingeschränkten Bewegungsfähigkeit oder Sehbehinderung, damit sie informationstechnologische Inhalte erfolgreich verwenden können.

Übersicht

Die IBM Power Systems-Server umfassen folgende Hauptfunktionen zur barrierefreien Bedienung:

- Bedienung nur über die Tastatur
- Vorgänge, bei denen ein Sprachausgabeprogramm verwendet wird

Die IBM Power Systems-Server verwenden den aktuellen W3C-Standard, WAI-ARIA 1.0 (www.w3.org/TR/wai-aria/), um die Einhaltung von US Section 508 (www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) und Web Content Accessibility Guidelines (WCAG) 2.0 (www.w3.org/TR/WCAG20/) sicherzustellen. Um die Funktionen zur barrierefreien Bedienung nutzen zu können, verwenden Sie das aktuelle Release Ihres Sprachausgabeprogramms und den aktuellen Web-Browser, der von den IBM Power Systems-Servern unterstützt wird.

Die Online-Produktdokumentation zu IBM Power Systems-Servern im IBM Knowledge Center ist für die barrierefreie Bedienung aktiviert. Eine Beschreibung der Funktionen zur barrierefreien Bedienung im IBM Knowledge Center finden Sie unter dem Abschnitt "Accessibility" im Hilfebereich des IBM Knowledge Center (www.ibm.com/support/knowledgecenter/doc/kc_help.html#accessibility).

Tastaturnavigation

Dieses Produkt verwendet Standardnavigationstasten.

Schnittstelleninformationen

In den Benutzerschnittstellen der IBM Power Systems-Server gibt es keine Inhalte, die 2 bis 55 Mal pro Sekunde blinken.

Die Webbenutzerschnittstelle der IBM Power Systems-Server basiert auf Cascading Style Sheets, um Inhalte ordnungsgemäß wiederzugeben und positive Erfahrungen zu ermöglichen. Die Anwendung bietet eine funktional entsprechende Möglichkeit für Benutzer mit eingeschränktem Sehvermögen, um die Einstellungen für die Systemanzeige, einschließlich des Modus für kontraststarke Anzeige, zu verwenden. Sie können die Schriftgröße über die Einstellungen für die Einheit oder den Web-Browser steuern.

Die Webbenutzerschnittstelle für IBM Power Systems-Server umfasst WAI-ARIA-Navigationsmarkierungen, mit deren Hilfe Sie schnell zu Funktionsbereichen in der Anwendung navigieren können.

Software anderer Anbieter

Die IBM Power Systems-Server enthalten bestimmte Software anderer Anbieter, die nicht von der IBM Lizenzvereinbarung abgedeckt wird. IBM übernimmt keine Garantie für die Funktionen zur barrierefreien Bedienung dieser Produkte. Wenden Sie sich an den Anbieter, um Informationen zur barrierefreien Bedienung der entsprechenden Produkte zu erhalten.

Zugehörige Informationen zur barrierefreien Bedienung

Neben dem gewohnten IBM Helpdesk und den Support-Websites bietet IBM einen TTY-Telefonservice für gehörlose oder hörgeschädigte Kunden für den Zugriff auf Vertriebs- und Support-Services:

TTY-Service
800-IBM-3383 (800-426-3383)
(innerhalb von Nordamerika)

Weitere Informationen zum Engagement von IBM für barrierefreie Bedienung finden Sie unter IBM Accessibility (www.ibm.com/able).

Hinweise zur Datenschutzrichtlinie

IBM Softwareprodukte, einschließlich Software-as-a-service-Lösungen ("Softwareangebote"), können Cookies oder andere Technologien verwenden, um Informationen zur Produktnutzung zu erfassen, die Endbenutzererfahrung zu verbessern und Interaktionen mit dem Endbenutzer anzupassen oder zu anderen Zwecken. In vielen Fällen werden von den Softwareangeboten keine personenbezogenen Daten erfasst. Einige der IBM Softwareangebote können Sie jedoch bei der Erfassung personenbezogener Daten unterstützen. Wenn dieses Softwareangebot Cookies zur Erfassung personenbezogener Daten verwendet, sind nachfolgend nähere Informationen über die Verwendung von Cookies durch dieses Angebot zu finden.

Abhängig von den bereitgestellten Konfigurationen werden von diesem Softwareangebot Sitzungscookies zum Erfassen von Benutzernamen und IP-Adressen der einzelnen Benutzer für die Sitzungsverwaltung verwendet. Diese Cookies können inaktiviert werden, dadurch wird jedoch auch ihre Funktionalität inaktiviert.

Wenn die für dieses Softwareangebot genutzten Konfigurationen Sie als Kunde in die Lage versetzen, personenbezogene Daten von Endbenutzern über Cookies und andere Technologien zu erfassen, müssen Sie sich zu allen gesetzlichen Bestimmungen in Bezug auf eine solche Datenerfassung, einschließlich aller Mitteilungspflichten und Zustimmungsanforderungen, rechtlich beraten lassen.

Weitere Informationen zur Nutzung verschiedener Technologien, einschließlich Cookies, für diese Zwecke finden Sie in der IBM Datenschutzerklärung unter http://www.ibm.com/privacy und in der IBM Erklärung zum Onlinedatenschutz unter http://www.ibm.com/privacy/details/us/en/ im Abschnitt “Cookies, Web-Beacons und sonstige Technologien”.

Marken

IBM, das IBM Logo und ibm.com sind Marken oder eingetragene Marken der International Business Machines Corporation in den USA und/oder anderen Ländern. Weitere Produkt- und Servicenamen können Marken von IBM oder anderen Unternehmen sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite Copyright and trademark information.

Die eingetragene Marke Linux wird gemäß einer Unterlizenz von der Linux Foundation verwendet, dem ausschließlichen Lizenznehmer von Linus Torvalds, weltweit Eigentümer dieser Marke.

Red Hat, JBoss, OpenShift, Fedora, Hibernate, Ansible, CloudForms, RHCA, RHCE, RHCSA, Ceph und Gluster sind Marken oder eingetragene Marken der Red Hat, Inc. oder ihrer Tochtergesellschaften in den USA und anderen Ländern.

Microsoft und Windows sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

Java und alle auf Java basierenden Marken und Logos sind Marken oder eingetragene Marken der Oracle Corporation und/oder ihrer verbundenen Unternehmen.

Elektromagnetische Verträglichkeit

Hinweise für Geräte der Klasse A

Die folgenden Hinweise zur elektromagnetischen Verträglichkeit von Geräten der Klasse A beziehen sich auf IBM Server mit POWER9-Prozessor und auf deren Komponenten, es sei denn, diese sind in den zugehörigen Informationen als Geräte der Klasse B ausgewiesen.

Beim Anschließen eines Bildschirms an das Gerät müssen das dafür vorgesehene Bildschirmkabel und die mit dem Bildschirm bereitgestellten Entstörungseinheiten verwendet werden.

Canada Notice

CAN ICES-3 (A)/NMB-3(A)

European Community and Morocco Notice

This product is in conformity with the protection requirements of Directive 2014/30/EU of the European Parliament and of the Council on the harmonization of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

This product may cause interference if used in residential areas. Such use must be avoided unless the user takes special measures to reduce electromagnetic emissions to prevent interference to the reception of radio and television broadcasts.

Warning: This equipment is compliant with Class A of CISPR 32. In a residential environment this equipment may cause radio interference.

Deutschsprachiger Hinweis

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 nur von 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 Funkstörungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen."

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem "Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)". Dies ist die Umsetzung der EU-Richtlinie 2014/30/EU in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC Richtlinie 2014/30/EU) für Geräte der Klasse A

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV-Vorschriften ist der Hersteller:
International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
Tel.: 914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:
IBM Deutschland GmbH
Technical Relations Europe, Abteilung M456
IBM-Allee 1, 71139 Ehningen, Deutschland
Tel.: +49 800 225 5426
E-Mail: HalloIBM@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022/EN 55032 Klasse A.

Japan Electronics and Information Technology Industries Association (JEITA) Notice

（一社）電子情報技術産業協会　高調波電流抑制対策実施
要領に基づく定格入力電力値： Knowledge Centerの各製品の
仕様ページ参照

This statement applies to products less than or equal to 20 A per phase.

高調波電流規格 JIS C 61000-3-2 適合品

This statement applies to products greater than 20 A, single phase.

高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。
• 回路分類 ：6（単相、ＰＦＣ回路付）
• 換算係数 ：0

This statement applies to products greater than 20 A per phase, three-phase.

高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。
- 回路分類 ：5（3相、ＰＦＣ回路付）
- 換算係数 ：0

Japan Voluntary Control Council for Interference (VCCI) Notice

この装置は、クラスA 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI－A

Korea Notice

이 기기는 업무용 환경에서 사용할 목적으로 적합성평가를 받은 기기로서 가정용 환경에서 사용하는 경우 전파간섭의 우려가 있습니다.

People's Republic of China Notice

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。

Russia Notice

ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать
радиопомехи, для снижения которых необходимы
дополнительные меры

Taiwan Notice

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。

IBM Taiwan Contact Information:

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

United States Federal Communications Commission (FCC) Notice

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. Proper cables and connectors are available from IBM-authorized dealers. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:
(1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Responsible Party:
International Business Machines Corporation
New Orchard Road
Armonk, NY 10504
Contact for FCC compliance information only: fccinfo@us.ibm.com

Hinweise für Geräte der Klasse B

Die folgenden Hinweise zur elektromagnetischen Verträglichkeit von Geräten der Klasse B beziehen sich auf Komponenten, die in den zugehörigen Installationsinformationen als Geräte der Klasse B ausgewiesen sind.

Beim Anschließen eines Bildschirms an das Gerät müssen das dafür vorgesehene Bildschirmkabel und die mit dem Bildschirm bereitgestellten Entstörungseinheiten verwendet werden.

Canada Notice

CAN ICES-3 (B)/NMB-3(B)

European Community and Morocco Notice

This product is in conformity with the protection requirements of Directive 2014/30/EU of the European Parliament and of the Council on the harmonization of the laws of the Member States relating to electromagnetic compatibility. IBM cannot accept responsibility for any failure to satisfy the protection requirements resulting from a non-recommended modification of the product, including the fitting of non-IBM option cards.

Deutschsprachiger Hinweis

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 nur von 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, Deutschland
Tel.: +49 800 225 5426
E-Mail: HalloIBM@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55032 Klasse B

Japan Electronics and Information Technology Industries Association (JEITA) Notice

（一社）電子情報技術産業協会　高調波電流抑制対策実施
要領に基づく定格入力電力値：Knowledge Centerの各製品の
仕様ページ参照

This statement applies to products less than or equal to 20 A per phase.

高調波電流規格 JIS C 61000-3-2 適合品

This statement applies to products greater than 20 A, single phase.

高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。
• 回路分類 ：6（単相、ＰＦＣ回路付）
• 換算係数 ：0

This statement applies to products greater than 20 A per phase, three-phase.

高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。
• 回路分類 ：5（3相、ＰＦＣ回路付）
• 換算係数 ：0

Japan Voluntary Control Council for Interference (VCCI) Notice

この装置は，クラスB情報技術装置です。この装置は，家庭環境で使用することを目的としていますが，この装置がラジオやテレビジョン受信機に近接して使用されると，受信障害を引き起こすことがあります。
取扱説明書に従って正しい取り扱いをして下さい。 VCCI－B

Taiwan Notice

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

United States Federal Communications Commission (FCC) Notice

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult an IBM-authorized dealer or service representative for help.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. Proper cables and connectors are available from IBM-authorized dealers. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:

(1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Responsible Party:

International Business Machines Corporation
New Orchard Road
Armonk, New York 10504
Contact for FCC compliance information only: fccinfo@us.ibm.com

Nutzungsbedingungen

Die Berechtigungen zur Nutzung dieser Veröffentlichungen werden Ihnen auf der Basis der folgenden Bedingungen gewährt.

Anwendbarkeit: Die vorliegenden Bedingungen gelten zusätzlich zu den Nutzungsbedingungen für die Website von IBM.

Persönliche Nutzung: Sie dürfen diese Veröffentlichungen für Ihre persönliche, nicht kommerzielle Nutzung unter der Voraussetzung vervielfältigen, dass alle Eigentumsvermerke erhalten bleiben. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM weder weitergeben oder anzeigen noch abgeleitete Werke davon erstellen.

Kommerzielle Nutzung: Sie dürfen diese Veröffentlichungen nur innerhalb Ihres Unternehmens und unter der Voraussetzung, dass alle Eigentumsvermerke erhalten bleiben, vervielfältigen, weitergeben und anzeigen. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM außerhalb Ihres Unternehmens weder vervielfältigen, weitergeben oder anzeigen noch abgeleitete Werke davon erstellen.

Berechtigungen: Abgesehen von den hier gewährten Berechtigungen werden keine weiteren Berechtigungen, Lizenzen oder Rechte (veröffentlicht oder stillschweigend) in Bezug auf die Veröffentlichungen oder darin enthaltene Informationen, Daten, Software oder geistiges Eigentum gewährt.

IBM behält sich das Recht vor, die in diesem Dokument gewährten Berechtigungen nach eigenem Ermessen zurückzuziehen, wenn sich die Nutzung der Veröffentlichungen für IBM als nachteilig erweist oder wenn die obigen Nutzungsbestimmungen nicht genau befolgt werden.

Sie dürfen diese Informationen nur in Übereinstimmung mit allen anwendbaren Gesetzen und Vorschriften, einschließlich aller US-amerikanischen Exportgesetze und Verordnungen, herunterladen und exportieren.

IBM ÜBERNIMMT KEINE GEWÄHRLEISTUNG FÜR DEN INHALT DIESER VERÖFFENTLICHUNGEN. Diese Veröffentlichungen werden auf der Grundlage des gegenwärtigen Zustands (auf "as-is"-Basis) und ohne eine ausdrückliche oder stillschweigende Gewährleistung für die Handelsüblichkeit, die Verwendungsfähigkeit für einen bestimmten Zweck oder die Freiheit von Rechten Dritter zur Verfügung gestellt.