

Power Systems

Instalarea și configurarea consolei HMC



Notă

Înainte de a utiliza aceste informații și produsul la care se referă, citiți informațiile din “Observații privind măsurile de siguranță” la pagina v, “Observații” la pagina 97, manualul *IBM Systems Safety Notices*, G229-9054, și *IBM Environmental Notices and User Guide*, Z125-5823.

Această ediție este valabilă pentru IBM® Hardware Management Console Versiunea 9 Ediția 2 Nivelul de întreținere 950 și pentru toate edițiile și modificările următoare până când se indică altceva în noile ediții.

© Copyright International Business Machines Corporation 2018, 2021.

Cuprins

Observații privind măsurile de siguranță.....	V
Instalarea și configurarea Hardware Management Console.....	1
Ce este nou în Instalarea și configurarea consolei HMC.....	1
Taskurile de instalare și configurare.....	2
Instalarea și configurarea unei noi console HMC cu un server nou.....	2
Actualizarea și modernizarea codului HMC.....	3
Adăugarea unei a doua console HMC la o instalare existentă.....	3
Setarea consolei HMC.....	4
Instalarea IBM Power Systems HMC (7063-CR2) într-un dulap.....	4
Instalarea 7063-CR1 în dulap.....	13
Instalarea unui dispozitiv virtual HMC	23
Configurarea consolei HMC.....	36
Alegerea setărilor de rețea pe HMC.....	36
Configurarea consolei HMC.....	53
Pașii post-configurare.....	73
Actualizarea, modernizarea și migrarea codului de mașină al consolei HMC.....	74
Securizarea consolei HMC.....	85
Politica de parolă îmbunătățită.....	87
Profilurile de securitate: GDPR (Global Data Protection Regulation) și PCI-DSS (Payment Card Industry Data Security Standard)	88
Rezolvarea problemelor comune în timpul securizării HMC.....	90
Locațiile porturilor HMC.....	93
Observații.....	97
Caracteristicile de accesibilitate pentru serverele IBM Power Systems.....	98
Considerente privind politica de confidențialitate	99
Mărci comerciale.....	99
Observații privind emisia electronică.....	100
Observații privind Clasa A.....	100
Observații privind Clasa B.....	103
Termeni și condiții.....	106

Observații privind măsurile de siguranță

Pe parcursul acestui ghid pot apărea observații privind măsurile de siguranță:

- Observațiile **PERICOL** atrag atenția asupra unei situații care poate cauza moartea sau poate fi extrem de periculoasă pentru oameni.
- Observațiile **PRUDENTĂ** atrag atenția asupra unei situații care poate fi periculoasă pentru oameni din cauza unei condiții existente.
- Observațiile **ATENȚIE** vă cer atenția asupra unei posibile deteriorări a unui program, dispozitiv, sistem sau a datelor.

Informații privind măsurile de siguranță pentru comerțul internațional

În câteva țări este necesară prezentarea în limba națională a informațiilor privind măsurile de siguranță din publicațiile produsului. Dacă această cerință este valabilă pentru țara dumneavoastră, în pachetul cu publicații livrat împreună cu produsul este inclusă documentația cu informațiile privind măsurile de siguranță (ca materiale tipărite, pe DVD sau ca parte a produsului). Documentația conține informațiile privind măsurile de siguranță în limba dumneavoastră națională, cu referiri la sursa în limba engleză. Înainte de a utiliza o publicație în limba engleză americană pentru a instala, opera sau face service pentru acest produs, trebuie să vă familiarizați cu informațiile privind măsurile de siguranță din documentație. De asemenea, ar trebui să consultați documentația cu informații privind măsurile de siguranță ori de câte ori nu înțelegeți prea bine vreo informație privind măsurile de siguranță din publicațiile în limba engleză americană.

Pentru a obține copii noi sau suplimentare ale documentației cu informații privind măsurile de siguranță, sunați la IBM Hotline, la 1-800-300-8751.

Informații în germană privind măsurile de siguranță

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

Informații privind măsurile de siguranță pentru laser

Serverele IBM pot folosi plăci I/E sau caracteristici bazate pe fibre optice care utilizează laserul sau leduri.

Compatibilitatea privind laserul

Serverele IBM pot fi instalate în afara sau în interiorul unui dulap de echipamente IT.

Toate dispozitivele cu laser sunt certificate în Statele Unite cu privire la respectarea cerințelor specificate în subcapitolul J din DHHS 21 CFR pentru produsele cu laser din clasa 1. În afara Statelor Unite, sunt certificate pentru conformitatea cu IEC 60825 ca produs laser din clasa 1. Vedeți eticheta de pe fiecare parte componentă pentru numerele certificării referitoare la laser și informațiile despre aprobare.

Informații privind alimentarea și cablarea pentru NEBS (Network Equipment-Building System) GR-1089-CORE

Comentariile următoare sunt valabile pentru serverele IBM care au fost desemnate ca fiind conforme cu NEBS (Network Equipment-Building System) GR-1089-CORE:

Echipamentul este adecvat pentru instalarea în:

- Facilități de telecomunicații prin rețea
- Locații unde se aplică NEC (National Electrical Code)

Porturile de interior ale acestui echipament sunt adecvate numai pentru conectarea la cablajul intern, neexpus al clădirii. *Nu este permisă* conectarea metalică a porturilor de interior ale acestui echipament la

interfețe care se conectează la instalații exterioare sau la cablajul acestora. Aceste interfețe sunt concepute să fie folosite numai ca interfețe de interior (porturi Tip 2 sau Tip 4, după cum se arată în GR-1089-CORE) și trebuie să fie izolate față de cablajul expus al instalațiilor externe. Adăugarea unor siguranțe principale nu reprezintă o protecție suficientă pentru a conecta metalic aceste interfețe la cablajul instalațiilor externe.

Notă: Toate cablurile Ethernet trebuie să fie ecranate și legate la pământ în ambele capete.

Sistemul cu alimentare c.a. nu necesită utilizarea unui dispozitiv extern de protecție la supratensiune.

Sistemul cu alimentare c.c. folosește cablarea cu retur c.c. izolat (DC-I). *Nu este permisă* conectarea terminalului de retur al bateriei c.c. la legătura la pământ a șasiului sau a cadrului.

Sistemul cu alimentare c.c. este conceput pentru a fi instalat într-o rețea comună, după cum este descris în GR-1089-CORE.

Instalarea și configurarea Hardware Management Console

Aflați cum să instalați hardware-ul Hardware Management Console (HMC), să îl conectați la sistemul gestionat și să îl configurați pentru utilizare. Puteți realiza aceste taskuri singur sau puteți lua legătura cu un furnizor de servicii, pentru a le realiza în locul dumneavoastră. Este posibil ca furnizorul de servicii să vă perceapă o taxă pentru acest serviciu.

Ce este nou în Instalarea și configurarea consolei HMC

Aflați ce informații sunt noi sau modificate semnificativ în subiectul Instalarea și configurarea HMC, față de actualizarea anterioară a acestei colecții de subiecte.

Aprilie 2021

- Au fost adăugate următoarele subiecte:
 - [“Instalarea IBM Power Systems HMC \(7063-CR2\) într-un dulap”](#) la pagina 4
 - [“Cerințe preliminare pentru instalarea sistemului 7063-CR2 montat în dulap”](#) la pagina 4
 - [“Finalizarea inventarului pentru sistemul dumneavoastră”](#) la pagina 5
 - [“Determinarea și marcarea locației în dulap pentru sistemul 7063-CR2”](#) la pagina 5
 - [“Atașarea șinelor ajustabile la șasiul sistemului și la dulap”](#) la pagina 6
 - [“Atașarea șinelor fixe pe șasiul sistemului și pe dulap”](#) la pagina 8
 - [“Instalarea sistemului în dulap și conectarea și pozarea cablurilor de alimentare”](#) la pagina 9
 - [“Cablaarea consolei HMC 7063-CR2 montate în dulap”](#) la pagina 10
 - [“Configurarea consolei HMC 7063-CR2”](#) la pagina 11

Noiembrie 2020

- Au fost actualizate subiectele următoare:
 - [“Taskurile de instalare și configurare”](#) la pagina 2
 - [“Securizarea consolei HMC”](#) la pagina 85
 - [“Locațiile porturilor HMC”](#) la pagina 93

Iulie 2020

- Au fost actualizate subiectele următoare:
 - [“Instalarea unui dispozitiv virtual HMC ”](#) la pagina 23
 - [“Locațiile porturilor HMC”](#) la pagina 93

Octombrie 2019

- Au fost actualizate subiectele următoare:
 - [“Instalarea unui dispozitiv virtual HMC ”](#) la pagina 23
 - [“Securizarea consolei HMC”](#) la pagina 85

Februarie 2019

- Au fost adăugate următoarele subiecte:

- [“Securizarea consolei HMC” la pagina 85](#)
- [“Politica de parolă îmbunătățită” la pagina 87](#)
- [“Rezolvarea problemelor comune în timpul securizării HMC” la pagina 90](#)
- [“Profilurile de securitate: GDPR \(Global Data Protection Regulation\) și PCI-DSS \(Payment Card Industry Data Security Standard\) ” la pagina 88](#)

August 2018

- Au fost actualizate subiectele următoare:
 - [“Configurarea consolei HMC 7063-CR1” la pagina 20](#)
 - [“Locațiile porturilor HMC” la pagina 93](#)

Decembrie 2017

- Au fost adăugate informații pentru serverele IBM Power Systems care conțin procesoare POWER9.

Taskurile de instalare și configurare

Aflați mai multe despre diferite taskuri asociate cu instalarea și configurarea consolei HMC.

Această secțiune descrie, la nivel înalt, taskurile pe care trebuie să le realizați când instalați și configurați consola HMC. Există diverse moduri în care puteți instala și configura consola HMC. Găsiți cea mai potrivită situație pentru taskul pe care doriți să-l realizați.

Note:

- Dacă gestionați servere bazate pe POWER9 consola HMC trebuie să fie la Versiunea 9.1.0 sau ulterioară. Pentru informații suplimentare, vedeți [“Determinarea versiunii și ediției codului de mașină HMC” la pagina 75](#).
- Nu se acceptă Hardware Management Console Versiunea 9.2.950 sau ulterioară pentru tipul de mașină HMC 7042. Pentru informații suplimentare despre versiunile HMC pentru consola dumneavoastră HMC 7042, vedeți notele de ediție pentru HMC, care sunt disponibile pe site-ul web [Fix Central](#).

Instalarea și configurarea unei noi console HMC cu un server nou

Aflați despre taskurile de nivel înalt pe care trebuie să le realizați la instalarea și configurarea unei noi console HMC cu un server nou.

<i>Tabela 1. Taskurile pe care trebuie să le realizați la instalarea și configurarea unei noi console HMC cu un server nou</i>	
Task	Unde puteți găsi informații înrudite
1. Adunați informații și finalizați foaia de lucru Configurare preinstalare.	“Foaia de lucru pentru configurarea dinaintea instalării HMC” la pagina 46 “Pregătirea pentru configurarea consolei HMC” la pagina 44
2. Despachetați hardware-ul.	
3. Cablați hardware-ul consolei HMC.	“Cablați consolei HMC 7063-CR1 montate în dulap” la pagina 18
4. Porniți consola HMC apăsând butonul de alimentare.	
5. Logați-vă și lansați aplicația web consolă HMC.	

Tabela 1. Taskurile pe care trebuie să le realizați la instalarea și configurarea unei noi console HMC cu un server nou (continuare)

Task	Unde puteți găsi informații înrudite
6. Accesați vrăjitorul Guided Setup sau folosiți meniurile consolei HMC pentru a configura consola HMC.	“Configurarea HMC utilizând calea rapidă prin vrăjitorul Guided Setup” la pagina 53 “Configurarea HMC folosind meniurile ” la pagina 53
7. Atașați serverul la consola HMC.	

Actualizarea și modernizarea codului HMC

Aflați mai multe despre taskurile de nivel înalt pe care trebuie să le realizați când actualizați și modernizați codul consolei HMC.

Dacă aveți o consolă HMC și vreți să actualizați sau să modernizați codul consolei HMC, trebuie să finalizați următoarele taskuri de nivel înalt:

Tabela 2. Taskurile pe care trebuie să le realizați la actualizarea sau modernizarea codului consolei HMC

Task	Unde puteți găsi informații înrudite
1. Obțineți modernizarea.	“Modernizarea software-ului HMC” la pagina 80
2. Vizualizați nivelul codului de mașină HMC existent.	
3. Salvați datele de profil ale sistemului gestionat.	
4. Salvați datele consolei HMC.	
5. Înregistrați informațiile curente ale configurației HMC.	
6. Înregistrați starea la distanță a comenzii.	
7. Salvați datele de modernizare.	
8. Modernizați software-ul consolei HMC.	
9. Verificați dacă modernizarea codului de mașină HMC a fost instalată cu succes	

Adăugarea unei a doua console HMC la o instalare existentă

Aflați mai multe despre taskurile de nivel înalt pe care trebuie să le realizați la adăugarea unei a doua console HMC la sistemul gestionat.

Dacă aveți o consolă HMC existentă și un sistem gestionat și vreți să adăugați o a doua consolă HMC la această configurație, faceți următoarele:

Tabela 3. Taskurile pe care trebuie să le realizați la adăugarea unei a doua console HMC la o instalare existentă

Task	Unde puteți găsi informații înrudite
1. Asigurați-vă că hardware-ul consolei HMC suportă cod de consolă HMC versiunea 7.	
2. Adunați informații și finalizați foaia de lucru Configurare preinstalare.	“Foaia de lucru pentru configurarea dinaintea instalării HMC” la pagina 46
3. Despachetați hardware-ul.	

Tabela 3. Taskurile pe care trebuie să le realizați la adăugarea unei a doua console HMC la o instalare existentă (continuare)

Task	Unde puteți găsi informații înrudite
4. Cablați hardware-ul consolei HMC.	“Cablaarea consolei HMC 7063-CR1 montate în dulap” la pagina 18
5. Porniți consola HMC apăsând butonul de alimentare.	
6. Logați-vă în consola HMC.	
7. Nivelurile de cod HMC trebuie să se potrivească. Schimbați codul de pe o consolă HMC pentru a se potrivi cu codul de pe cealaltă.	“Determinarea versiunii și ediției codului de mașină HMC” la pagina 75 “Modernizarea software-ului HMC” la pagina 80
8. Accesați vrăjitorul Guided Setup sau folosiți meniurile consolei HMC pentru a configura consola HMC.	“Configurarea HMC folosind meniurile ” la pagina 53
9. Configurați această consolă HMC pentru service folosind vrăjitorul Call-Home Setup.	“Configurarea consolei HMC pentru a se conecta la organizația de service și suport folosind vrăjitorul de setare call-home” la pagina 67
10. Atașați serverul la consola HMC.	

Setarea consolei HMC

Trebuie să setați consola HMC înainte de a configura software-ul HMC. Aflați detalii despre setarea unei console HMC desk-side sau a unei console HMC montate în dulap.

Instalarea IBM Power Systems HMC (7063-CR2) într-un dulap

Aflați cum se instalează IBM Power Systems HMC (7063-CR2) într-un dulap.

Puteți vizualiza online documentația de instalare sau puteți tipări versiunea PDF a acelorași informații. Pentru a vizualiza sau tipări versiunea PDF, vedeți [Instalarea și configurarea Hardware Management Console](#).

Cerințe preliminare pentru instalarea sistemului 7063-CR2 montat în dulap

Utilizați informațiile pentru a înțelege cerințele preliminare care sunt necesare pentru instalarea sistemului.

Despre acest task

Poate fi necesar să citiți următoarele documente înainte de a începe să instalați serverul:

- Cea mai recentă versiune a acestui document este actualizată online, vedeți [Installing the 7063-CR2 into a rack](http://www.ibm.com/support/knowledgecenter/POWER9/p9hai/p9hai_install7063cr2_kickoff.htm) (http://www.ibm.com/support/knowledgecenter/POWER9/p9hai/p9hai_install7063cr2_kickoff.htm).
- Pentru a vă planifica instalarea serverului, vedeți [Planificarea locației și hardware-ului](#).

Procedură

1. Asigurați-vă că aveți următoarele articole înainte de a începe instalarea dumneavoastră:
 - Șurubelniță cu cap cruce mărimea 2
 - Șurubelniță cu cap plat

- Șurubelniță T25
- Cutter de cutii
- Brățară de descărcare electrostatică (ESD)
- Dulap cu spațiu de o unitate EIA (Electronic Industries Association) (1U)

Note:

- Dacă nu aveți instalat un dulap, instalați dulapul. Pentru instrucțiuni, vedeți Dulapuri și caracteristici de dulapuri (http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_9xx_kickoff.htm).
- Caracteristicile sursei de alimentare sunt 100 la 127 V c.a, 9 A (x2), 200 la 240 V c.a, 4.5 A (x2); 50 sau 60 Hz.

2. Continuați cu “Finalizarea inventarului pentru sistemul dumneavoastră” la pagina 5.

Finalizarea inventarului pentru sistemul dumneavoastră

Folosiți aceste informații pentru a finaliza inventarul pentru sistemul dumneavoastră.

Procedură

1. Verificați dacă ați primit toate cutiile pe care le-ați comandat.
2. Despachetați componentele serverului după cum este necesar.
3. Finalizați un inventar și verificați că ați primit toate părțile componente comandate înainte de a instala fiecare componentă de server.

Notă:

Informațiile pentru comanda dumneavoastră sunt incluse cu produsul dumneavoastră. De asemenea puteți obține informațiile de la reprezentantul de marketing sau de la partenerul de afaceri IBM.

Dacă aveți părți componente incorecte, lipsă sau deteriorate, consultați oricare dintre următoarele resurse:

- Reseller-ul IBM.
 - Linia IBM Rochester Manufacturing Automated Information Line, la 1-800-300-8751 (numai în Statele Unite).
 - Site-ul web Directory of worldwide contacts (<http://www.ibm.com/planetwide>). Selectați locația dumneavoastră pentru a vizualiza informațiile de contact ale organizației de service și suport.
4. Continuați cu “Determinarea și marcarea locației în dulap pentru sistemul 7063-CR2” la pagina 5.

Determinarea și marcarea locației în dulap pentru sistemul 7063-CR2

Trebuie să determinați unde să instalați unitatea de sistem în dulap.

Procedură

1. Citiți Observații asupra măsurilor de siguranță pentru dulap (http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_racksafety.htm).
2. Determinați unde să amplasați unitatea de sistem în dulap. Pe măsură ce planificați instalarea unității de sistem într-un dulap, luați în considerare următoarele informații:
 - Organizați unitățile mai mari și mai grele în partea de jos a dulapului.
 - Planificați instalarea unităților de sistem începând cu partea de jos a dulapului.
 - Înregistrați locațiile Electronic Industries Alliance (EIA) în planul dumneavoastră.
3. Dacă este necesar, înlăturați panourile de umplutură, pentru a permite accesul în interiorul incintei dulapului, acolo unde intenționați să amplasați unitatea, după cum se arată în Figura 1 la pagina 6.

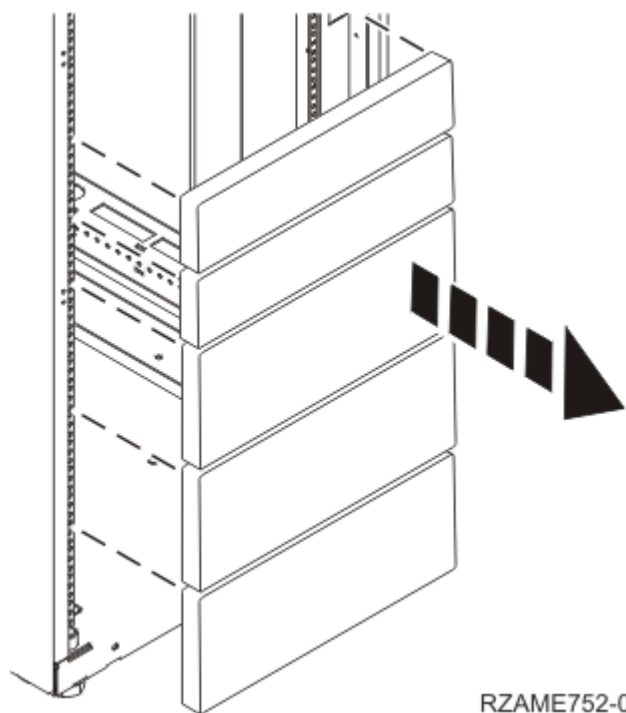


Figura 1. Înlăturarea panourilor de umplură

4. Determinați unde să plasați sistemul în dulap. Notați poziția EIA.
5. Stând cu fața la dulap și lucrând din partea dreaptă, utilizați bandă, un marcaj sau creion pentru a marca orificiul inferior al fiecărei unități EIA.
6. Repetați pasul "5" la pagina 6 pentru orificiile corespundente din partea stângă a dulapului.
7. Mutați-vă în spatele dulapului.
8. În partea din dreapta, găsiți unitatea EIA care corespunde unității EIA de jos marcate în fața dulapului.
9. Marcați unitatea EIA de jos.
10. Marcați orificiile corespundente din partea stângă a dulapului.
11. Continuați cu "Atașarea șinelor ajustabile la șasiul sistemului și la dulap" la pagina 6 pentru a atașa șinele ajustabile sau continuați cu "Atașarea șinelor fixe pe șasiul sistemului și pe dulap" la pagina 8 pentru a atașa șinele fixe.

Atașarea șinelor ajustabile la șasiul sistemului și la dulap

Trebuie să instalați șinele pe șasiu și în dulap. Utilizați această procedură pentru a finaliza acest task.

Despre acest task



Atenție: Pentru a evita defectarea șinei și un pericol potențial pentru dumneavoastră și pentru unitate, asigurați-vă că aveți șinele și garniturile corecte pentru dulapul dumneavoastră. Dacă dulapul dumneavoastră are orificii pătrate în flanșa de suport sau orificii în șir pentru șuruburi, asigurați-vă că șinele și garniturile se potrivesc cu orificiile flanșei de suport care sunt folosite pe dulapul dumneavoastră. Nu instalați hardware nepotrivit folosind șaibe sau distanțiere. Dacă nu aveți șine și accesorii corespunzătoare pentru dulapul dumneavoastră, contactați reseller-ul IBM.

Notă: Unitățile EIA din dulapuri sunt măsurate în incremente verticale de 44,45 mm (1,75 inch.) fiecare. Fiecare increment de 44,45 mm (1,75 inch) este numit un "EIA." În unele țări, același increment este numit un "U".

Notă: Sistemul necesită o unitate de dulap cu spațiu de 1 EIA (1U).

Asigurați-vă că aveți părțile componente necesare pentru a instala șinele. Următoarele părți componente sunt incluse în kitul de șine:

- 4 - șuruburi cu cap cruce de 6,35 mm (0,25 inch)
- 2 - ansambluri șină de colțare dulap și glisieră
- 2 - colțare de glisieră HMC
- 10 - piulițe colivie pentru găuri de montare EIA pătrate
- 10 - piulițe colivie pentru găuri de montare EIA rotunde
- 10 - șuruburi hexagonale M5 cu flanșă

Procedură

- Scoateți piesele șinelor din pachet și puneți-le pe o suprafață de lucru.
- Identificați spațiul de 1U din dulapul consolei HMC.
- Pentru a atașa colțarele de glisieră la HMC, realizați următoarele taskuri:
 - Identificați colțarul de glisieră dreapta.
 - Aliniați găurile de pe colțarul de glisieră dreapta cu pinii colțarului de glisieră aflați pe partea dreaptă a stației de lucru HMC. Asigurați-vă că toți pinii sunt aliniați cu găurile colțarului.
 - Împingeți colțarul glisierei HMC înspre partea din spate a stației de lucru HMC până când se blochează complet în poziție.
 - Fixați colțarul glisierei din dreapta pe partea dreaptă a stației de lucru HMC cu două șuruburi cu cap cruce de 6,35 mm (0,25 inch) introduse în găurile de șurub.
 - Repetăți pașii “3.a” la pagina 7 - “3.d” la pagina 7 pentru a instala colțarul de glisare din stânga în partea stângă a stației de lucru HMC.
- Mutați-vă către partea frontală a dulapului.
 - Pe partea stângă, puneți trei piulițe colivie în cele trei găuri a marginii din față a dulapului în slotul de 1U care este desemnat pentru HMC.

Notă: Kitul de șine include piulițe colivie atât pentru găurile rotunde, cât și pentru găurile pătrate. Asigurați-vă că folosiți piulițe colivie corespunzătoare găurilor din dulap.
 - Repetăți pasul “4.a” la pagina 7 în partea dreaptă a dulapului.
- Mutați-vă în spatele dulapului.
 - Pe partea stângă, puneți două piulițe colivie în gaura de sus și de jos găuri a marginii din față a dulapului în slotul de 1U care este desemnat pentru HMC.

Notă: Gaura din mijloc trebuie să rămână goală.
 - Repetăți pasul “5.a” la pagina 7 în partea dreaptă a dulapului.
- Pentru a instala șinele de glisare HMC în dulap, realizați următorii pași:
 - Măsurați adâncimea dulapului. Adâncimea trebuie să fie între 558,8 mm (22 inch) și 863,6 mm (34 inch).
 - Plasați șinele de glisare pe o suprafață plată și găsiți șuruburile preinstalate.

Notă: Șinele de glisare au patru găuri de șurub.
 - Slăbiți șuruburile preinstalate de pe șinele de glisare, astfel încât șinele să se poată mișca ușor spre interior sau spre exterior.
 - Pe baza adâncimii dulapului măsurată în pasul “6.a” la pagina 7, trebuie să reglați șuruburile pe șine.
 - Dacă adâncimea dulapului este între 558,8 mm (22 inch) și 698,5 mm (27.5 inch), puneți șuruburile în prima și a treia gaură.
 - Dacă adâncimea dulapului este între 698,5 mm (27.5 inch) și 863,6 mm (34 inch), puneți șuruburile în doua și a patra gaură.

Note:

- Prima gaură este întotdeauna cea mai aproape de capătul șinei de glisare. Gaura a treia și a patra sunt aproape una de alta.
 - Asigurați-vă că șuruburile nu sunt așa de strânse, astfel încât lungimea șinei să poate fi ajustată ușor la instalarea în dulap.
7. În partea din față a dulapului, instalați în dulap șinele de glisare pentru HMC prin realizarea următorilor pași:
 - a. Găsiți ansamblul șinei de glisare din stânga.
 - b. Orientați ansamblul de șină astfel încât capătul cu cea mai aproape gaură (prima gaură) să intre la început în dulap. Asigurați-vă că stau cu fața la dulap capetele șuruburilor. Slotul deschis al ansamblului șinei este mai aproape de partea din față a dulapului.
 - c. În partea stângă a dulapului, conectați flanșa de la capătul șinei de glisare la marginea din față a dulapului prin două șuruburi M5, lăsând gaura din mijloc goală. Asigurați-vă că ansamblul șinei este nu este strâns prea tare pe partea din față a dulapului pentru a permite introducerea stației de lucru HMC.
 8. În partea din spate a dulapului, în partea dreaptă, trageți capătul liber al șinei de glisare către partea din spate și prindeți flanșa șinei de glisare la dulap folosind două șuruburi M5, lăsând gaura din mijloc goală.
 9. Repetați pasul "7" la [pagina 8](#) și pasul "8" la [pagina 8](#) pentru a instala ansamblul șinei de glisare din dreapta pe partea dreaptă a dulapului.
 10. În partea din față a dulapului, instalați stația de lucru HMC prin realizarea următorilor pași:
 - a. Păstrând nivelul stației de lucru HMC, inserați colțarele de glisare în șinele de glisare pentru HMC pe care le-ați instalat în pasul anterior. Împingeți HMC înainte până când flanșele de pe partea din față a HMC sunt aliniate cu orificiile de șurub goale de pe partea din față a dulapului.
 - b. Prindeți HMC de partea din stânga a cadrului cu un șurub M5. Repetați acest pas în partea dreaptă a dulapului.
 11. Continuați cu ["Instalarea sistemului în dulap și conectarea și pozarea cablurilor de alimentare"](#) la [pagina 9](#).

Atașarea șinelor fixe pe șasiul sistemului și pe dulap

Trebuie să instalați șinele pe șasiu și în dulap. Utilizați această procedură pentru a finaliza acest task.

Despre acest task



Atenție: Pentru a evita defectarea șinei și un pericol potențial pentru dumneavoastră și pentru unitate, asigurați-vă că aveți șinele și garniturile corecte pentru dulapul dumneavoastră. Dacă dulapul dumneavoastră are orificii pătrate în flanșa de suport sau orificii în șir pentru șuruburi, asigurați-vă că șinele și garniturile se potrivesc cu orificiile flanșei de suport care sunt folosite pe dulapul dumneavoastră. Nu instalați hardware nepotrivit folosind șaibe sau distanțiere. Dacă nu aveți șine și accesorii corespunzătoare pentru dulapul dumneavoastră, contactați reseller-ul IBM.

Notă: Unitatea 1 EIA este măsurată în dulapuri în incremente verticale de 1,75 inch. fiecare. Fiecare increment de 44,45 mm (1,75 inch) este numit un "EIA." În unele țări, același increment este numit un "U".

Notă: Sistemul necesită o unitate de dulap cu spațiu de 1 EIA (1U).

Asigurați-vă că aveți părțile componente necesare pentru a instala șinele. Următoarele părți componente sunt incluse în kitul de șine:

- 4 - șuruburi cu cap cruce de 6,35 mm (0,25 inch)
- 2 - șine interioare
- 2 - șine de suport HMC
- 2 - piulițe colivie pentru găuri de montare EIA pătrate
- 2 - piulițe colivie pentru găuri de montare EIA rotunde

- 8 - șuruburi hexagonale M5 cu flanșă

Procedură

1. Scoateți piesele șinelor din pachet și puneți-le pe o suprafață de lucru.
2. Identificați spațiul de 1U din dulapul consolei HMC.
3. Pentru a atașa șinele interioare la HMC, realizați următoarele taskuri:
 - a. Identificați șina interioară din dreapta.
 - b. Aliniați găurile de pe șina interioară dreapta cu pinii șinei aflați pe partea dreaptă a stației de lucru HMC. Asigurați-vă că toți pinii sunt aliniați cu găurile șinei interioare.
 - c. Împingeți șina interioară HMC înspre partea din față a stației de lucru HMC până când se blochează complet în poziție.
 - d. Fixați colțarul șinei interioare din dreapta pe partea dreaptă a stației de lucru HMC cu două șuruburi cu cap cruce de 6,35 mm (0,25 inch) introduse în găurile de șurub.
 - e. Repetați pașii 3.a - “3.d” la [pagina 9](#) pentru a instala șina interioară din stânga în partea stângă a stației de lucru HMC.

4. Mutați-vă către partea frontală a dulapului. Pe partea stângă, puneți o piuliță colivie în gaura marginii din față a dulapului în slotul de 1U care este desemnat pentru HMC.

Notă: Kitul de șine include piulițe colivie atât pentru găurile rotunde, cât și pentru găurile pătrate. Asigurați-vă că folosiți piulițe colivie corespunzătoare găurilor din dulap.

5. Mutați-vă în spatele dulapului. Pe partea stângă, puneți o piuliță colivie în gaura din mijloc marginii din față a dulapului în slotul de 1U care este desemnat pentru HMC.
6. În partea din față a dulapului, instalați în dulap șinele de suport HMC prin realizarea următorilor pași:
 - a. Aliniați pinii șinelor de suport deasupra și dedesubtul piuliței colivie pe care ați instalat-o în pasul anterior.
 - b. În partea dreaptă a dulapului, conectați flanșa de la capătul șinei de suport la marginea din față a dulapului prin două șuruburi M5, în gaura de sus și de jos, lăsând gaura din mijloc goală. Asigurați-vă că ansamblul șinei este nu este strâns prea tare pe partea din față a dulapului pentru a permite introducerea stației de lucru HMC.
7. În partea din spate a dulapului, în partea dreaptă, trageți capătul liber al șinei de suport către partea din spate și prindeți flanșa șinei la dulap folosind două șuruburi M5, lăsând gaura din mijloc goală.
8. Repetați pasul “6” la [pagina 9](#) și pasul “7” la [pagina 9](#) pentru a instala ansamblul șinei de suport din stânga pe partea stângă a dulapului.
9. În partea din față a dulapului, instalați stația de lucru HMC prin realizarea următorilor pași:
 - a. Păstrând nivelul stației de lucru HMC, inserați șinele interioare în șinele de suport pentru HMC pe care le-ați instalat în pasul anterior. Împingeți HMC înainte până când flanșele de pe partea din față a HMC sunt aliniate cu orificiile de șurub goale de pe partea din față a dulapului.
 - b. Prindeți HMC de partea din stânga a cadrului cu un șurub M5. Repetați acest pas în partea dreaptă a dulapului.

Notă: Dacă sunt prezente, înlăturați colțarele pentru transport portocalii care sunt prinse în spatele sistemului și apoi prindeți șurubul înapoï.

10. Continuați cu [“Instalarea sistemului în dulap și conectarea și pozarea cablurilor de alimentare” la pagina 9.](#)

Instalarea sistemului în dulap și conectarea și pozarea cablurilor de alimentare

După ce instalați sistemul la șine, conectați și pozați cablurile de alimentare.

Despre acest task

Procedură

1. Scoateți stratul protectiv de plastic din partea de sus a șasiului sistemului.
2. Atașați cabloanele de alimentare la sursele de alimentare.

Notă: Nu conectați celălalt capăt al cablului de alimentare la sursa de alimentare acum.

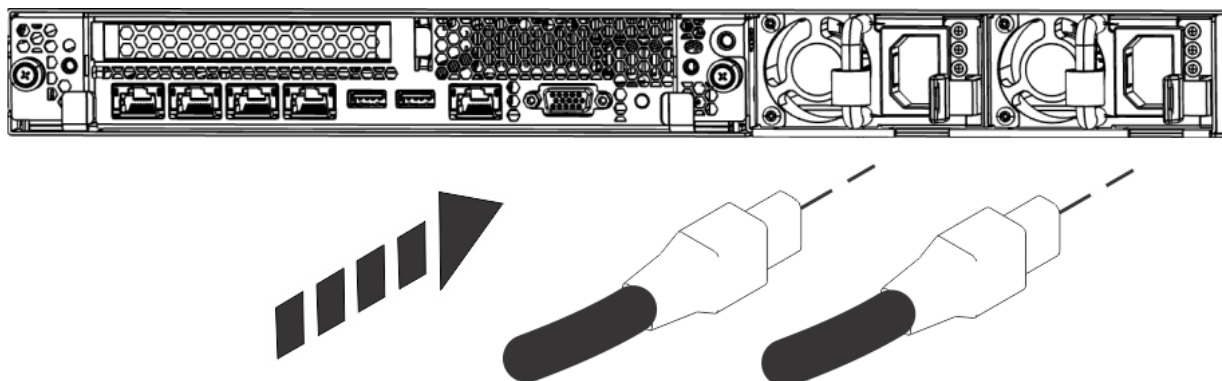


Figura 2. Atașarea cabloanelor de alimentare la sursele de alimentare

3. Strângeți elementele de fixare babă-moș pentru a securiza cabloanele de alimentare.
4. Continuați cu [“Cablaarea consolei HMC 7063-CR2 montate în dulap”](#) la pagina 10.

Cablarea consolei HMC 7063-CR2 montate în dulap

Aflați cum se instalează fizic consola HMC (Hardware Management Console) montată în dulap.

Procedură

1. Asigurați-vă că consola HMC este instalată într-un dulap și că cabloanele de alimentare sunt atașate la sursele de alimentare. Pentru informații suplimentare, vedeți [“Instalarea sistemului în dulap și conectarea și pozarea cablurilor de alimentare”](#) la pagina 9. După ce instalați HMC într-un dulap, continuați cu pasul următor.
2. Conectați tastatura, monitorul și mouse-ul.

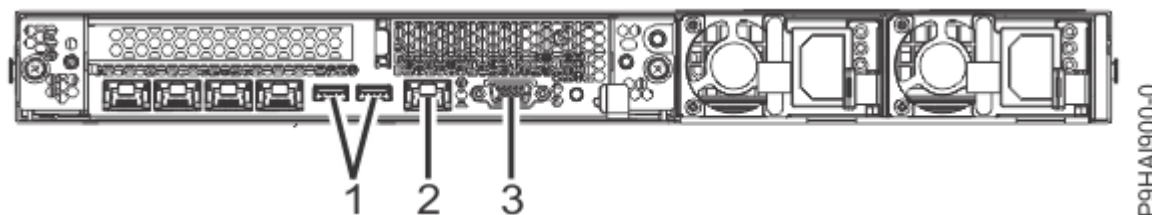


Figura 3. Porturi spate

Tabela 4. Porturi de intrare și de ieșire	
Identificator	Descriere
1	USB 2.0 folosit pentru tastatură și mouse
2	Ethernet Intelligent Platform Management Interface (IPMI)
3	Video Graphics Array (VGA), utilizat pentru monitor. Este suportată numai setarea 1024 x 768 la 60 Hz VGA. Este suportat numai un cablu de până la 3 metri.

Notă: Sistemul are două porturi USB frontale pe care le puteți utiliza.

3. Conectați portul Ethernet Intelligent Platform Management Interface (IPMI) la o rețea.

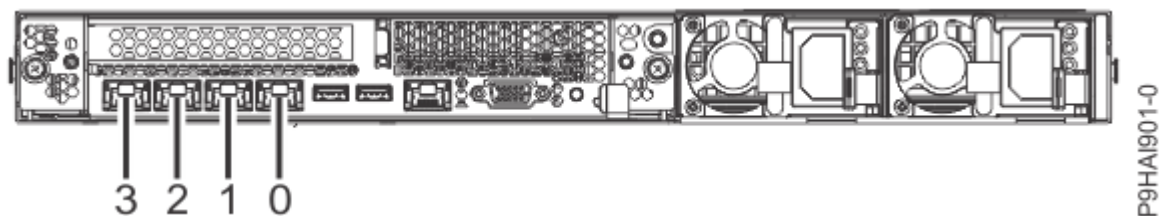


Figura 4. Porturile Ethernet

Tabela 5. Porturile Ethernet	
Identificator	Descriere
0	Conexiunea de rețea Ethernet partajată IPMI (Intelligent Platform Management Interface) și HMC
1, 2 și 3	Conexiune de rețea HMC

Notă: Această conexiune este necesară pentru a accesa controlerul de gestionare a plăcii de bază (baseboard management controller - BMC), pe HMC. Accesul la BMC este necesar pentru taskurile de service și pentru a menține firmware-ul HMC. Pentru informații suplimentare, vedeți [“Tipurile de conexiuni de rețea HMC”](#) la pagina 37.

Avertisment: Este posibil ca acest produs să nu fie certificat în țara dumneavoastră pentru conectarea prin orice mijloace la interfețele rețelelor publice de telecomunicații. Pentru a realiza o astfel de conexiune, legislația poate impune o certificare suplimentară. Vă rugăm să contactați IBM pentru mai multe informații.

4. Conectați cablul Ethernet destinat conexiunii la sistemul sau sistemele gestionate.

Note:

- Dacă utilizați o conexiune partajată pentru IPMI și HMC, un singur cablu la portul 0 din Figura 2 poate satisface ambele cerințe pentru IPMI și HMC.
 - Pentru a afla mai multe despre conexiunile de rețea ale consolei HMC, consultați [“Conexiunile de rețea HMC”](#) la pagina 36.
5. Dacă sistemul dumneavoastră gestionat este deja instalat, puteți verifica dacă este activă conexiunea cablului Ethernet observând ledurile de stare verzi de la porturile Ethernet ale consolei HMC și ale sistemului gestionat, pe măsură ce instalarea progresează.
 6. Conectați cablurile de alimentare ale sistemului și cablurile de alimentare pentru toate celelalte dispozitive atașate în sursa de alimentare de curent alternativ (AC).
 7. Verificați starea alimentării folosind ca indicatoare ledurile de pe sursa de alimentare. Pentru informații suplimentare, vedeți [LED-urile pe sistemul 7063-CR2](#) și [LED-uri pe sistemul 7063-CR2](#).
 8. Apăsați butonul de alimentare pentru a porni sistemul. Indicatorul luminos de punere sub tensiune nu mai este iluminat intermitent și rămâne aprins, indicând că alimentarea sistemului este pornită.

Rezultate

Apoi, trebuie să vă instalați și să configurați software-ul de HMC. Continuați cu [“Configurarea consolei HMC 7063-CR2”](#) la pagina 11.

Configurarea consolei HMC 7063-CR2

Aflați cum se instalează și se configurează consola HMC (Hardware Management Console).

Verificați versiunea de HMC livrată pentru consola dumneavoastră HMC. Pentru a afla cum puteți să vizualizați versiunea și ediția codului de mașină HMC, vedeți [Verificarea versiunii HMC care este livrată cu](#)

consola HMC. Puteți descărca cea mai recentă versiune de HMC disponibilă de pe site-ul web Fix Central. Utilizați un mediu de stocare amovibil (cum ar fi un DVD sau USB) pentru a crea un fișier ISO de boot din pachetul HMC (imaginea ISO).

Notă: Următorul tabel descrie informațiile predefinite (implicite) de logare pentru interfețele HMC și BMC.

Tabela 6.			
Consola sau interfața	ID implicit	Parolă implicită	Descriere
BMC (OpenBMC)	root	0penBmc	ID-ul de utilizator root și parola sunt folosite pentru a se loga la BMC pentru prima dată.
HMC	hscroot	abc123	ID-ul și parola utilizatorului hscroot sunt folosite pentru prima logare la HMC. Sunt sensibile la majuscule și pot fi folosite doar de către un membru al rolului super administrator.
HMC	root	passw0rd	ID-ul și parola utilizatorului root sunt folosite de către furnizorul de servicii pentru a realiza proceduri de întreținere. Nu pot fi utilizate pentru logarea la HMC.

Notă: Următoarele instalări sunt afișate ca exemple.

Instalarea HMC folosind unitatea flash pentru USB

Pentru a instala consola HMC folosind unitatea flash USB, parcurgeți pașii următori pentru sistemele Linux®:

Notă: Pentru exemple în diferite sisteme de operare, consultați:

- Windows: [USB flash installation media \(Windows\)](#)
- Mac: [USB flash installation media \(macOS\)](#)

1. Descărcați versiunea de HMC pe care o doriți din site-ul web [Fix Central](#).
2. Rulați comanda următoare: **dd bs=4M if=/path/to/HMC_ISO_FILE.iso of=/dev/sdx status=progress && sync** (unde **sdx** este numele unității USB).

Notă: Puteți rula comanda Linux `lsblk` pentru a determina numele de dispozitiv al drive-ului USB când este conectat.

3. Inserați unitatea USB și puneți sistemul sub tensiune.

Notă: Unitatea USB trebuie să aibă cel puțin 8 GB. Anumite unități USB pot să fie prea late pentru a se potrivi corespunzător în portul USB din spatele sistemului. Testați dacă unitatea dumneavoastră USB se potrivește înainte de a continua.

4. Atunci când este afișat meniul Petitboot, selectați opțiunea **Install Hardware Management Console** care este localizată sub **USB**.

Instalarea consolei HMC folosind medii virtuale de la BMC

Pentru a instala consola HMC folosind mediul virtual de pe BMC, parcurși următorii pași:

1. Deschideți un browser web suportat. În bara de adresă, introduceți adresa IP pentru BMC la care vreți să vă conectați. De exemplu, puteți utiliza formatul `https://<IP BMC>` în bara de adresă a browser-ului web.
2. Din fereastra **OpenBMC logon**, introduceți adresa **Host** pentru BMC și **Username** și **Password** alocate dumneavoastră.

Notă: ID-ul de logare implicit este `root`, iar parola implicită este `OpenBmc`.

Dacă utilizați nivelul de firmware OP940.01, sau ulterior, parola pentru root expiră implicit. Trebuie să schimbați parola implicită înainte de a accesa BMC. Pentru informații suplimentare despre schimbarea parolei implicite, [Setarea parolei](#).

Dacă ați uitat parola, puteți realiza o resetare la setările din fabrică a sistemului pentru a restaura la parola implicită. Pentru a reseta sistemul, vedeți [Realizarea unei resetări la setările din fabrică](#).

3. Faceți clic pe **Log in**.
4. Selectați **Server control**.
5. Selectați **Virtual Media**.
6. Faceți clic pe **Choose file**.
7. Găsiți HMC Recovery media ISO și faceți clic pe **Open**.
8. Faceți clic pe **Start**.
9. Porniți sistemul.
10. Atunci când este afișat meniul Petitboot, selectați opțiunea **Install Hardware Management Console** care este localizată sub **USB**.

Instalarea HMC folosind o unitate DVD externă conectată prin USB

Pentru a instala HMC folosind o unitate DVD externă conectată prin USB, parcurgeți pașii următori:

1. Descărcați versiunea de recuperare HMC pe care o doriți de pe site-ul web [Fix Central](#).
2. Ardeți imaginea DVD-ului de recuperare HMC la un mediu de stocare DVD-R DL ca imagine.
3. Opriți consola HMC.
4. Conectați unitatea DVD externă conectată prin USB la HMC și inserați DVD-ul de recuperare.

Notă: Este posibil să fie necesară conectarea unității DVD USB la o sursă de alimentare externă sau să folosiți un cablu USB Y pentru conexiunea la un port USB extra, pentru a furniza o putere suficientă unității DVD.

5. Porniți alimentarea consolei HMC.

Notă: Este posibil ca ecranul monitorului să nu aibă semnal în timpul pornirii consolei. Procesul poate dura 2 sau 3 minute până când ecranul monitorului va afișa o stare.

6. Atunci când pornește încărcătorul pentru boot Petitboot, navigați pentru a opri operația de boot automată.

Notă: Este impus un timeout de 10 secunde. Dacă nu are loc nici o acțiune în 10 secunde, sistemul încearcă să facă boot de pe hard disc.

7. Așteptați până când dispozitivul **CD/DVD** apare în meniul Petitboot.

Notă: Acest proces poate dura până la un minut.

8. Selectați opțiunea **Install Hardware Management Console** care este localizată sub **CD/DVD**.

Instalarea 7063-CR1 în dulap

Aflați cum se instalează într-un dulap consola HMC 7063-CR1.

Puteți vizualiza online documentația de instalare sau puteți tipări versiunea PDF a acestor informații. Pentru a vizualiza sau tipări versiunea PDF, vedeți [Instalarea și configurarea Hardware Management Console](#).

Cerințe preliminare pentru instalarea sistemului 7063-CR1 montat în dulap

Utilizați informațiile pentru a înțelege cerințele preliminare care sunt necesare pentru instalarea sistemului.

Despre acest task

Poate fi necesar să citiți următoarele documente înainte de a începe să instalați serverul:

- Cea mai recentă versiune a acestui document este menținută online, vedeți [Instalarea 7063-CR1 într-un dulap](http://www.ibm.com/support/knowledgecenter/POWER9/p9hai/p9hai_install7063_kickoff.htm) (http://www.ibm.com/support/knowledgecenter/POWER9/p9hai/p9hai_install7063_kickoff.htm).
- Pentru a vă planifica instalarea serverului, vedeți [Planificarea locației și hardware-ului](#).

Procedură

Asigurați-vă că aveți următoarele articole înainte de a începe instalarea dumneavoastră:

- Șurubelniță cu cap cruce mărimea 2
- Șurubelniță cu cap plat
- Cutter de cutii
- Brățară de descărcare electrostatică (ESD)
- Dulap cu spațiu de o unitate EIA (Electronic Industries Association) (1U)

Notă: Dacă nu aveți instalat un dulap, instalați dulapul. Pentru instrucțiuni, vedeți [Dulapuri și caracteristici de dulapuri](http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_9xx_kickoff.htm) (http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_9xx_kickoff.htm).

Finalizarea inventarului pentru sistemul dumneavoastră

Folosiți aceste informații pentru a finaliza inventarul pentru sistemul dumneavoastră.

Procedură

1. Verificați dacă ați primit toate cutiile pe care le-ați comandat.
2. Despachetați componentele serverului după cum este necesar.
3. Finalizați un inventar și verificați că ați primit toate părțile componente comandate înainte de a instala fiecare componentă de server.

Notă:

Informațiile pentru comanda dumneavoastră sunt incluse cu produsul dumneavoastră. De asemenea, puteți obține informațiile de la reprezentantul de marketing sau de la partenerul de afaceri IBM.

Dacă aveți părți componente incorecte, lipsă sau deteriorate, consultați oricare dintre următoarele resurse:

- Reseller-ul IBM.
- Linia IBM Rochester Manufacturing Automated Information Line, la 1-800-300-8751 (numai în Statele Unite).
- Site-ul web [Directory of worldwide contacts](http://www.ibm.com/planetwide) (<http://www.ibm.com/planetwide>). Selectați locația dumneavoastră pentru a vizualiza informațiile de contact ale organizației de service și suport.

Determinarea și marcarea locației în dulap pentru sistemul 7063-CR1

Poate fi necesar să stabiliți unde să fie instalată unitatea de sistem în dulap.

Procedură

1. Citiți Observații asupra măsurilor de siguranță pentru dulap (http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_racksafety.htm).
2. Determinați unde să amplasați unitatea de sistem în dulap. Pe măsură ce planificați instalarea unității de sistem într-un dulap, luați în considerare următoarele informații:
 - Organizați unitățile mai mari și mai grele în partea de jos a dulapului.
 - Planificați instalarea unităților de sistem începând cu partea de jos a dulapului.
 - Înregistrați locațiile Electronic Industries Alliance (EIA) în planul dumneavoastră.
3. Dacă este necesar, înlăturați panourile de umplutură, pentru a permite accesul în interiorul incintei dulapului, acolo unde intenționați să amplasați unitatea, după cum se arată în Figura 5 la pagina 15.

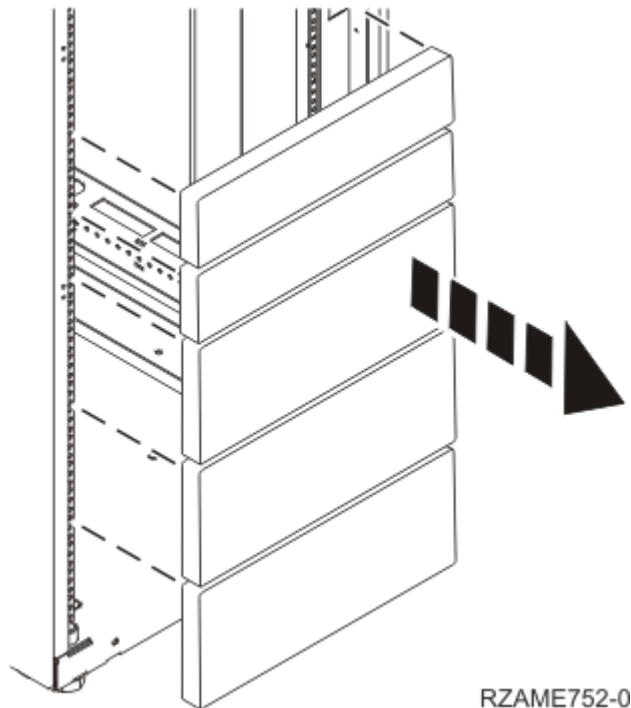


Figura 5. Înlăturarea panourilor de umplutură

4. Determinați amplasarea sistemului în dulap. Notați poziția EIA.
5. Stând cu fața la dulap și lucrând din partea dreaptă, utilizați bandă, un marcaj sau creion pentru a marca orificiul inferior al fiecărei unități EIA.
6. Repetați pasul “5” la pagina 15 pentru orificiile corespundente din partea stângă a dulapului.
7. Mutați-vă în spatele dulapului.
8. În partea din dreapta, găsiți unitatea EIA care corespunde unității EIA de jos marcate în fața dulapului.
9. Marcați unitatea EIA de jos.
10. Marcați orificiile corespundente din partea stângă a dulapului.

Atașarea șinelor fixe pe șasiul sistemului și pe dulap

Trebuie să instalați șinele pe șasiu și în dulap. Utilizați această procedură pentru a finaliza acest task.

Despre acest task



Atenție: Pentru a evita defectarea șinei și un pericol potențial pentru dumneavoastră și pentru unitate, asigurați-vă că aveți șinele și garniturile corecte pentru dulapul dumneavoastră. Dacă dulapul dumneavoastră are orificii pătrate în flanșa de suport sau orificii în șir pentru șuruburi, asigurați-vă că șinele și garniturile se potrivesc cu orificiile flanșei de suport care sunt folosite pe

dulapul dumneavoastră. Nu instalați hardware nepotrivit folosind șaibe sau distanțiere. Dacă nu aveți șine și accesorii corespunzătoare pentru dulapul dumneavoastră, contactați reseller-ul IBM.

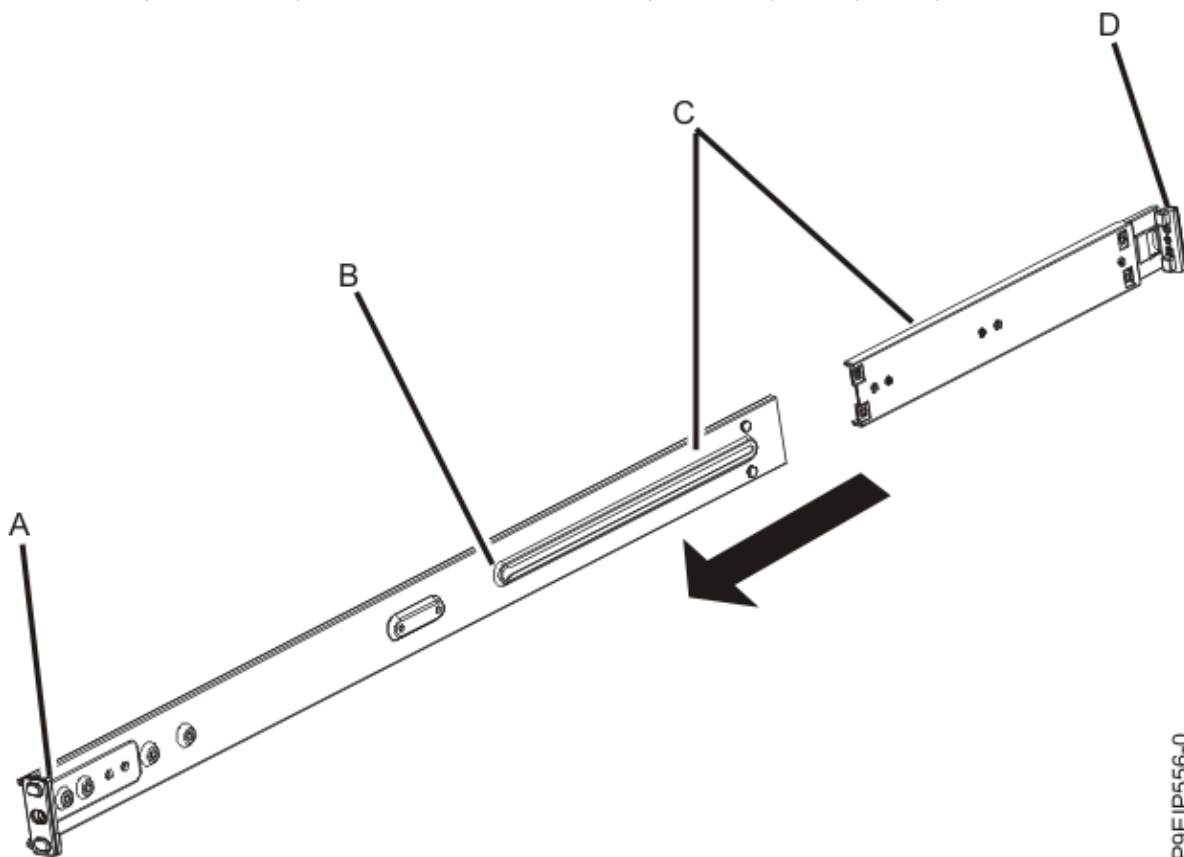
Notă: Sistemul necesită o unitate de dulap cu spațiu de 1 EIA (1U).

Asigurați-vă că aveți părțile componente necesare pentru a instala șinele. Următoarele părți componente sunt incluse în kitul de șine:

- Șuruburi de șine de glisare, folosite pentru a uni cele două părți ale fiecărei șine de glisare
- Șuruburi de dulap pentru șinele de glisare, folosite pentru a fixa șinele în dulap
- Șine
- Șuruburi 10 - 32 x 0,635 cm (0,25 inch), folosite pentru atașarea șinelor la șasiul sistemului

Procedură

1. Scoateți piesele șinelor din pachet și puneți-le pe o suprafață de lucru.
2. Înlocuiți pinii pătrați (A) și (D) ai dulapului cu pinii rotunzi.
3. Conectați cele două părți ale fiecărei șine de glisare de pe dulap. Pentru a conecta cele două părți ale șinei de glisare de pe dulap, realizați următoarele taskuri:
 - a. Identificați cele două piese ale șinei de glisare de pe dulap din stânga. Aliniați piesele scurte și lungi (C). Asigurați-vă că pinii șinei de pe dulap sunt orientați în aceeași direcție (A) și (D).



- b. Piesa scurtă a șinei de glisare de pe dulap are un pin de metal. Inserați pinul în orificiul din piesa mai lungă din șina de glisare de pe dulap (B). Glisați piesa scurtă a șinei de glisare de pe dulap în piesa mai lungă din șina de glisare de pe dulap.
- c. Aliniați orificiile din cele două piese ale șinelor de glisare de pe dulap. Folosind o șurubelniță cap cruce, atașați cele două părți înșurubând lejer două șuruburi prin orificiile din șina de glisare de pe dulap.

Notă: Nu strângeți șuruburile șinelor de glisare de pe dulap.

P9EIP556-0

- d. Repetați acești pași pentru șina de glisare dreapta.
4. Instalați în dulap șinele de glisare.
- a. Mutați-vă către partea frontală a dulapului.
 - b. Selectați șina de glisare de dulap stânga și localizați unitatea EIA marcată anterior. Fiecare șină de glisare este, de asemenea, marcată **Back**, pentru a desemna spatele dulapului. Asigurați-vă că țineți de capătul frontal al șinei de glisare de dulap.
 - c. Extindeți șina din partea frontală a dulapului către spate și aliniați pinii șinei cu orificiile din flanșa dulapului marcate anterior.
 - d. Împingeți pinii șinei de dulap în flanșa din spate până când zăvorul șinei spate de dulap face clic la locul ei.
 - e. Trageți partea din față a șinei de dulap către partea din față a flanșei de șină de dulap. Aliniați pinii șinei cu orificiile din flanșa șinei și trageți-le până când zăvorul șinei face clic la locul ei.
 - f. Folosind o șurubelniță, strângeți șuruburile șinei pe care ați instalat-o în pasul 2.
- Notă:** Este posibil să aveți nevoie de două unități de spațiu (2U) pentru a accesa și strânge șuruburile șinei.
- g. Repetați pașii 4a - 4f pentru șina de glisare dreapta.

Instalarea sistemului în dulap și conectarea și pozarea cablurilor de alimentare

După ce instalați sistemul la șine, conectați și pozați cablurile de alimentare.

Despre acest task

Procedură

1. Scoateți stratul protectiv de plastic din partea de sus a șasiului sistemului.
2. Mutați-vă către partea frontală a dulapului.
3. Împreună cu o altă persoană, ridicați sistemul și aliniați șinele de pe șasiul de sistem pe fiecare parte a șasiului cu șinele de glisare de pe dulap.
4. Împingeți încet sistemul către spatele dulapului.
5. Securizați sistemul de dulap înșurubând câte un șurub cu șaibă prin mânere, pe fiecare parte a șasiului sistemului.

Notă: Trebuie să utilizați șuruburile împreună cu șaibe. Puneți câte o șaibă pe fiecare dintre cele două șuruburi lungi (1,5 cm (0.59 inch)) care sunt incluse în kitul pentru șină. Înșurubați șurubul cu șaibă în stânga și dreapta părții frontale a sistemului.

6. Atașați cordonul de alimentare la sursele de alimentare.

Notă: Nu conectați celălalt capăt al cablului de alimentare la sursa de alimentare acum.

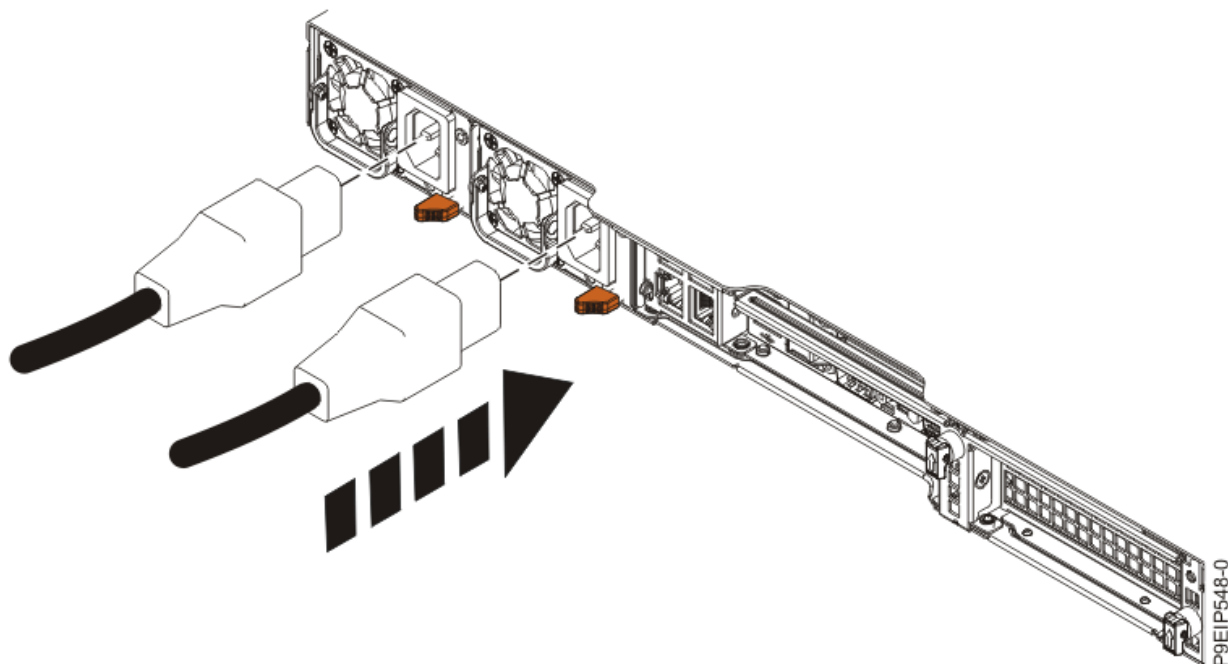


Figura 6. Atașarea cabloanelor de alimentare la sursele de alimentare

7. Continuați cu [“Cablaarea consolei HMC 7063-CR1 montate în dulap”](#) la pagina 18.

Cablarea consolei HMC 7063-CR1 montate în dulap

Aflați cum se instalează fizic consola HMC (Hardware Management Console) montată în dulap.

Procedură

1. Asigurați-vă că consola HMC este instalată într-un dulap și că cabloanele de alimentare sunt atașate la sursele de alimentare. Pentru informații suplimentare, vedeți [“Instalarea sistemului în dulap și conectarea și pozarea cablurilor de alimentare”](#) la pagina 17. După ce instalați HMC într-un dulap, continuați cu pasul următor.

Notă: Dacă există vreo fișă ce acoperă un port pe care trebuie să-l folosiți din spatele sistemului, înlăturați-o și aruncați-o. Acoperirea porturilor are rolul de a vă reaminti că trebuie să resetați parola de administrator pe sistemul dumneavoastră gestionat când se efectuează IPL (initial system load).

2. Conectați tastatura, monitorul și mouse-ul.

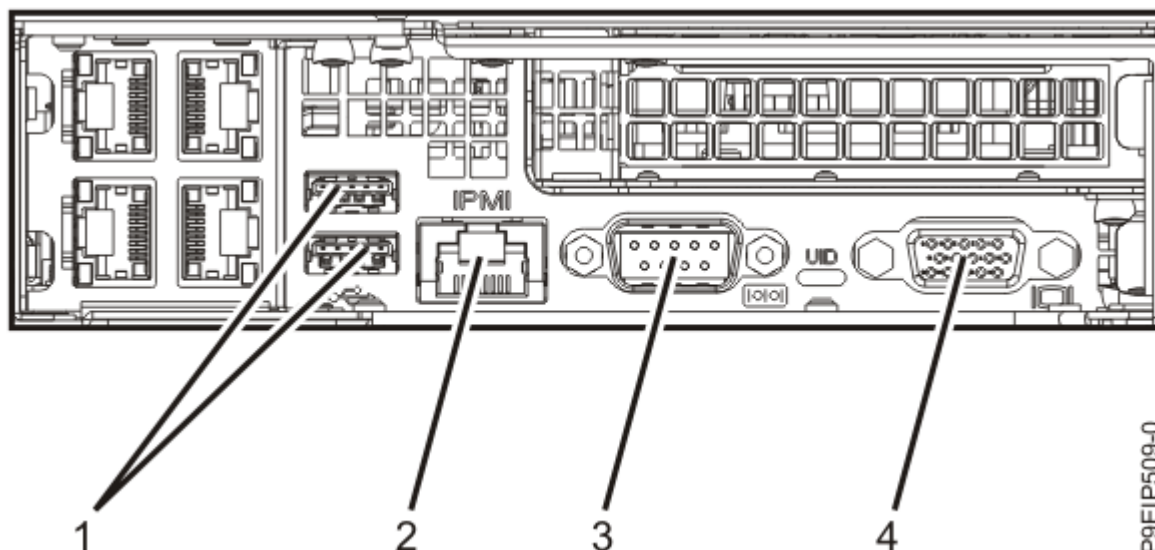


Figura 7. Porturi spate

Tabela 7. Porturi de intrare și de ieșire	
Identificator	Descriere
1	USB 2.0 folosit pentru tastatură și mouse
2	Ethernet Intelligent Platform Management Interface (IPMI)
3	IPMI serial
4	Video Graphics Array (VGA), utilizat pentru monitor. Este suportată numai setarea 1024 x 768 la 60 Hz VGA. Este suportat numai un cablu de până la 3 metri.

Notă: Sistemul are două porturi USB frontale pe care le puteți utiliza. Portul serial frontal nu este funcțional.

3. Conectați cablul Ethernet destinat conexiunii la sistemul sau sistemele gestionate.

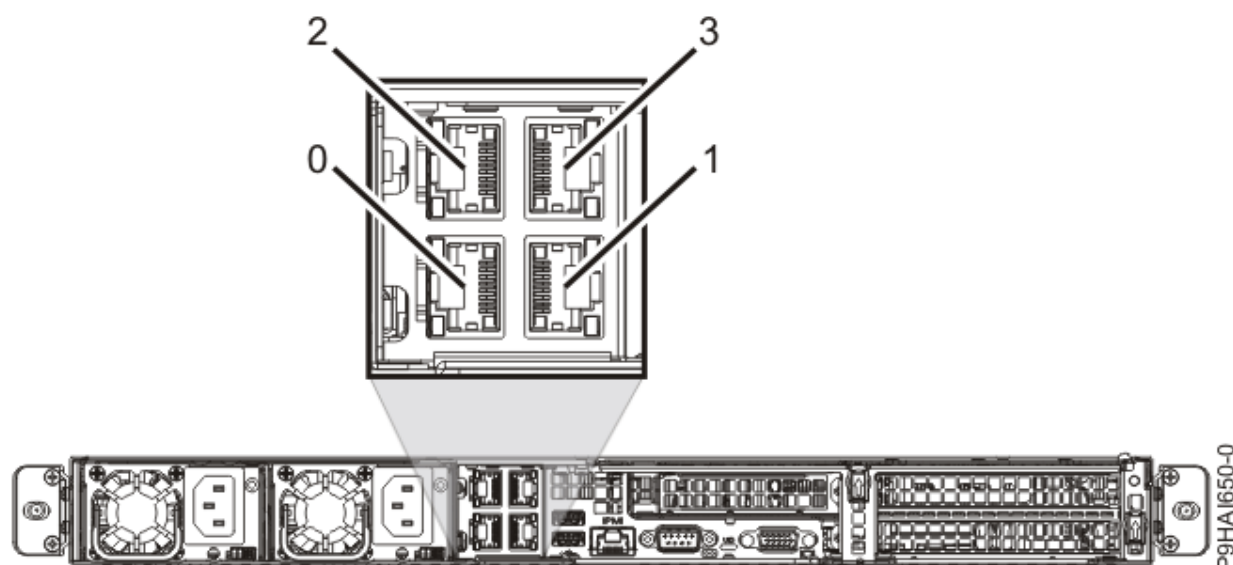


Figura 8. Porturile Ethernet

Notă: Pentru a afla mai multe despre conexiunile de rețea ale consolei HMC, consultați [“Conexiunile de rețea HMC”](#) la pagina 36.

4. Dacă sistemul dumneavoastră gestionat este deja instalat, puteți verifica dacă este activă conexiunea cablului Ethernet observând ledurile de stare verzi de la porturile Ethernet ale consolei HMC și ale sistemului gestionat, pe măsură ce instalarea progresează.
5. Conectați portul Ethernet Intelligent Platform Management Interface (IPMI) la o rețea.

Notă: Această conexiune este necesară pentru a accesa controlerul de gestionare a plăcii de bază (baseboard management controller - BMC), pe HMC. Accesul la BMC este necesar pentru taskurile de service și pentru a menține firmware-ul HMC. Pentru informații suplimentare, vedeți [“Tipurile de conexiuni de rețea HMC”](#) la pagina 37.

6. Conectați cablurile de alimentare ale sistemului și cablurile de alimentare pentru toate celelalte dispozitive atașate în sursa de alimentare de curent alternativ (AC).
7. Verificați starea alimentării folosind ca indicatoare ledurile de pe sursa de alimentare. Pentru informații suplimentare, vedeți [Ledurile pe sistemul 7063-CR1](#) și [Ledurile pe sistemul 7063-CR1](#).

Rezultate

Apoi, trebuie să vă instalați și să configurați software-ul de HMC. Continuați cu [“Configurarea consolei HMC 7063-CR1”](#) la pagina 20.

Configurarea consolei HMC 7063-CR1

Aflați cum se instalează și se configurează consola HMC (Hardware Management Console).

Verificați versiunea de HMC livrată pentru consola dumneavoastră HMC. Puteți descărca cea mai recentă versiune de HMC disponibilă de pe site-ul web [Fix Central](#). Utilizați un mediu de stocare amovibil (cum ar fi un DVD sau USB) pentru a crea un fișier ISO de boot din pachetul HMC (imaginea ISO).

Notă: Următorul tabel descrie informațiile predefinite (implicite) de logare pentru interfețele HMC și BMC.

Tabela 8.			
Consola sau interfața	ID implicit	Parolă implicită	Descriere
BMC	ADMIN	ADMIN	ID-ul și parola utilizatorului ADMIN sunt folosite pentru prima logare la BMC.
HMC	hscroot	abc123	ID-ul și parola utilizatorului hscroot sunt folosite pentru prima logare la HMC. Sunt sensibile la majuscule și pot fi folosite doar de către un membru al rolului super administrator.
HMC	root	passw0rd	ID-ul și parola utilizatorului root sunt folosite de către furnizorul de servicii pentru a realiza proceduri de întreținere. Nu pot fi utilizate pentru logarea la HMC.

Notă: Următoarele instalări sunt afișate ca exemple.

Instalarea HMC folosind unitatea flash pentru USB

Pentru a instala consola HMC folosind unitatea flash USB, parcurgeți pașii următori pentru sistemele Linux:

Notă: Pentru exemple în diferite sisteme de operare, consultați:

- Windows: [USB flash installation media \(Windows\)](#)
- Mac: [USB flash installation media \(macOS\)](#)

1. Descărcați versiunea de HMC pe care o doriți din site-ul web [Fix Central](#).
2. Rulați comanda următoare: **dd bs=4M if=/path/to/HMC_ISO_FILE.iso of=/dev/sdx status=progress && sync** (unde **sdx** este numele unității USB).

Notă: Puteți rula comanda Linux `lsblk` pentru a determina numele de dispozitiv al drive-ului USB când este conectat.

3. Inserați unitatea USB și puneți sistemul sub tensiune.

Notă: Unitatea USB trebuie să fie de cel puțin 4 GB. Este posibil ca anumite unități USB să fie prea late pentru a se potrivi corespunzător în portul USB din spatele sistemului. Testați dacă unitatea dumneavoastră USB se potrivește înainte de a continua.

4. Atunci când este afișat meniul Petitboot, selectați opțiunea **Install Hardware Management Console** care este localizată sub **USB**.

Instalarea HMC folosind mediul de stocare de la distanță de pe vizualizatorul consolei

Pentru a instala consola HMC folosind mediul de la distanță de pe vizualizatorul consolei, parcurgeți pașii următori:

1. Logați-vă la interfața web a BMC (<http://<bmc-ip>>).
2. Selectați **Remote Control**.
3. Selectați **Console Redirection**.
4. Faceți clic pe **Launch Console**.
5. În Java™ iKVM Viewer, selectați **Virtual Media > Virtual Storage**.
6. Sub **Logical Drive Type**, selectați **ISO File**.
7. Faceți clic pe **Open Image** și localizați fișierul ISO pe sistemul dumneavoastră.
8. Apăsați **Plugin** pentru a monta fișierul ISO.
9. Porniți sistemul.
10. Atunci când este afișat meniul Petitboot, selectați opțiunea **Install Hardware Management Console** care este localizată sub **CD/DVD**.

Instalarea HMC folosind o unitate DVD externă conectată prin USB

Pentru a instala HMC folosind o unitate DVD externă conectată prin USB, parcurgeți pașii următori:

1. Descărcați versiunea de recuperare HMC pe care o doriți de pe site-ul web [Fix Central](#).
2. Ardeți imaginea DVD de recuperare a consolei HMC pe un mediu de stocare DVD-R ca imagine. Alternativ, puteți comanda mediul de recuperare pe DVD.
3. Opriți consola HMC.
4. Conectați unitatea DVD externă conectată prin USB la HMC și inserați DVD-ul de recuperare.

Notă: Este posibil să fie necesară conectarea unității DVD USB la o sursă de alimentare externă sau să folosiți un cablu USB Y pentru conexiunea la un port USB extra, pentru a furniza o putere suficientă unității DVD.

5. Porniți alimentarea consolei HMC.

Notă: Este posibil ca ecranul monitorului să nu aibă semnal în timpul pornirii consolei. Procesul poate dura 2 sau 3 minute până când ecranul monitorului va afișa o stare.

6. Atunci când pornește încărcătorul pentru boot Petitboot, navigați pentru a opri operația de boot automată.

Notă: Este impus un timeout de 10 secunde. Dacă nu are loc nici o acțiune în 10 secunde, sistemul încearcă să facă boot de pe hard disc.

7. Așteptați până când dispozitivul **CD/DVD** apare în meniul Petitboot.

Notă: Acest proces poate dura până la un minut.

8. Selectați opțiunea **Install Hardware Management Console** care este localizată sub **CD/DVD**.

Instalarea HMC folosind mediul de stocare de la distanță care este găzduit pe un server de fișier SMB

Pentru instalarea HMC folosind mediul de stocare de la distanță care este găzduit pe un server de fișier SMB, parcurgeți pașii următori:

1. Copiați fișierul de recuperare ISO pe o gazdă partajată pe serverul dumneavoastră de fișier compatibil SMB.

Notă: Server Message Block versiunea 3 (SMBv3) nu este suportat.

2. Logați-vă la interfața web a BMC (<http://<bmc-ip>>).

3. Selectați **Virtual Media**.

4. Selectați **CD-ROM Image**.

5. Completați următoarele informații:

Share host

IP-ul gazdei SMB. Dacă folosiți numele de gazdă, asigurați-vă că sistemul de nume de domeniu (DNS) pe BMC este configurat corect.

Path to image

Calea SMB la sistem. De exemplu: `/<share name>/<rest of path>/<name of iso>.iso`

User (optional)

Numele de utilizator care este folosit pentru a vă loga la gazda SMB.

Password (optional)

Parola pentru utilizator.

6. Faceți clic pe **Save**.

7. Faceți clic pe **Mount**.

8. Dispozitivul 1 afișează acum următoarele mesaje: **There is an iso file mounted**.

Notă: Dacă nu apare mesajul, reverificați informațiile și repetați pașii [6](#) - [8](#).

9. Porniți sistemul.

10. Atunci când este afișat meniul Petitboot, selectați opțiunea **Install Hardware Management Console** care este localizată sub **CD/DVD**.

Opțional: Actualizarea nivelului de firmware HMC folosind stick-ul de memorie USB inclus

Notă: Dacă în configurația dumneavoastră este inclusă o actualizare de firmware HMC pe un stick de memorie USB, finalizați pașii următori pentru a actualiza nivelul firmware-ului HMC.

Pentru a actualiza nivelul firmware-ului HMC folosind stick-ul de memorie USB inclus, finalizați pașii următori:

1. Introduceți stick-ul de memorie USB în portul USB din spatele sistemului.
2. Porniți alimentarea sistemului și logați-vă pe consola HMC.

3. În zona de navigare, faceți clic pe pictograma **HMC Management**  și apoi selectați **Console Management**.
4. În panoul de conținut, apăsați pe **Update the Hardware Management Console**.
5. Urmăriți instrucțiunile de pe ecran ale vrăjitorului Install HMC Corrective Service.

Apoi, trebuie să vă configurați software-ul de HMC. Pentru instrucțiuni, consultați [“Configurarea consolei HMC” la pagina 36](#).

Concepte înrudite

[Configurarea conectivității BMC](#)

Puteți configura sau vizualiza setările de rețea de pe BMC pentru consola de gestionare.

Instalarea unui dispozitiv virtual HMC

Aflați cum se instalează un dispozitiv virtual Hardware Management Console (HMC).

Un dispozitiv virtual HMC poate fi instalat în infrastructura dumneavoastră existentă x86 sau POWER virtualizată. Un dispozitiv virtual HMC suportă următorii hipervizori de virtualizare x86:

- KVM (mașina virtuală bazată pe Kernel)
- Xen
- VMware

Un dispozitiv virtual HMC suportă următorii hipervizori de virtualizare POWER:

- PowerVM

Cerințele minime pentru rularea unui dispozitiv virtual HMC:

- 16 GB memorie
- 4 procesoare virtuale
- 2 interfețe de rețea (maxim 4 permise)
- 1 disc cu cel puțin 500 GB de spațiu disponibil.

Note:

- Pe sistemele care găzduiesc un dispozitiv virtual HMC, procesorul trebuie să fie un Intel VT-x sau un procesor AMD-V activat pentru virtualizare hardware.
- DVD-urile de dispozitiv virtual HMC pe care le primiți nu sunt pentru boot. Trebuie să montați mai întâi mediul și apoi să copiați fișierul .tgz din mediu. Metoda de montare a DVD-ului poate varia în funcție de sistemul de operare pe care îl utilizați.
- Sintaxa comenzilor folosite în exemplele următoare poate varia funcție de sistemul de operare pe care îl utilizați.
- Hipervizorul de virtualizare PowerVM necesită un spațiu de disc de 160 GB. Se recomandă însă o memorie de 500 GB.
- Procesorul PowerVM necesită cel puțin 1 unitate de procesare și 4 procesoare virtuale în modul de partajare acoperit. Nu se recomandă utilizarea procesoarelor dedicate. De asemenea, procesorul PowerVM necesită o memorie de 16 GB.

Informații înrudite

[Imagini de instalare în rețea a HMC V8 și instrucțiuni de instalare](#)

Instalarea unui dispozitiv virtual HMC pe x86

Aflați cum se instalează un dispozitiv virtual Hardware Management Console (HMC) într-un mediu x86.

Instalarea unui dispozitiv virtual HMC folosind hipervizorul KVM

Aflați cum se instalează un dispozitiv virtual Hardware Management Console (HMC) folosind hipervizorul de mașină virtuală bazată pe kernel (KVM).

Pentru a instala un dispozitiv virtual HMC pe KVM, parcurgeți pașii următori:

Notă: Pașii următori folosesc interfața linie de comandă și necesită autoritate de utilizator root. Sintaxa comenzilor poate varia în funcție de sistemul de operare.

1. Verificați că pachetele de virtualizare sunt instalate pe sisteme cu Red Hat Enterprise Linux (RHEL) versiunea 7.0 sau mai nouă.
2. Descărcați fișierul `<KVM vHMC installation filename>.tar.gz` pe sistemul gazdă.
3. Rulați comanda următoare `mkdir -p /var/lib/libvirt/images/vHMC`.
4. Rulați comanda următoare: `cd /var/lib/libvirt/images/vHMC`.
5. Pentru a extrage imaginile de disc virtual, rulați următoarea comandă: `tar -zxvf <KVM vHMC installation filename>.tgz`

Notă: În această comandă, specificați calea completă a fișierului dumneavoastră .tar de dispozitiv virtual HMC.

6. În fișierul `<KVM vHMC installation filename>.tar.gz` este furnizat un fișier **domain.xml**. Finalizați pașii următori:
 - a. Editați fișierul **domain.xml** și verificați că este corectă calea la discurile dumneavoastră. Fișierul conține șirul **DISK_PATH**.
 - b. Asigurați-vă că **virtio** este folosit în valoarea magistralei pentru dispozitivul discului dumneavoastră.
 - c. Puteți să alegeți un nume diferit pentru VM. Numele implicit în fișierul **domain.xml** este **vHMC**.
 - d. Verificați că adresa MAC (Media Access Control) este setată în fișierul **domain.xml**. Acest fișier conține șirul **MAC_ADDRESS**.

Notă: Înlăturați această linie dacă vreți ca o adresă MAC să fie generată pentru dumneavoastră.

- e. Verificați dacă punțile dumneavoastră se potrivesc cu dispozitivele dumneavoastră Ethernet. Fișierul implicit **domain.xml** specifică un Ethernet.
 - f. Dacă utilizați Activation Engine, înlocuiți **AEDISK** cu numele imaginii de disc virtual Activation Engine. Altfel, îndepărtați elementul de disc.
7. Pentru a defini mașina virtuală (VM), rulați comanda următoare: `virsh define <domain>.xml`.
 8. Pentru a verifica dacă consola HMC virtuală a fost adăugată în lista de mașini virtuale definite, rulați comanda următoare: `virsh list --all`.
 9. Pentru a porni VM, rulați comanda următoare: `virsh start vHMC`.
 10. Pentru a determina numărul de display VNC (Virtual Network Computing) pe consola dumneavoastră, rulați comanda următoare: `virsh vncdisplay vHMC`.
 11. Pentru a vă conecta la consola dumneavoastră cu un vizualizator VNC, rulați comanda următoare: `vncviewer HOSTNAME:ID` (Unde ID este numărul de display, de exemplu 0).

Notă: Dacă aveți nevoie de acces la distanță, trebuie să abandonați sau să configurați firewall-ul dumneavoastră pentru a permite accesul la portul 5900.

Instalarea unui dispozitiv virtual HMC folosind hipervizorul Xen

Aflați cum se instalează un dispozitiv virtual Hardware Management Console (HMC) folosind hipervizorul Xen.

Un dispozitiv virtual HMC suportă versiunea Xen 4.2 sau mai nouă.

Pentru a instala un dispozitiv virtual HMC folosind hipervizorul Xen, parcurgeți pașii următori:

Notă: Pașii următori utilizează interfața de linie de comandă și necesită autoritatea de utilizator root. Sintaxa comenzilor poate varia în funcție de sistemul de operare.

1. Verificați că pachetele de virtualizare sunt instalate pe sisteme cu Red Hat Enterprise Linux (RHEL) versiunea 6.4 sau mai nouă.
2. Descărcați fișierul <XEN vHMC installation filename>.tar.gz pe sistemul gazdă.
3. Rulați comanda următoare `mkdir -p /var/lib/libvirt/images/vHMC`.
4. Rulați comanda următoare: `cd /var/lib/libvirt/images/vHMC`.
5. Pentru a extrage imaginile de disc virtual, rulați următoarea comandă: `tar -zxvf <XEN vHMC installation filename>.tgz`

Notă: În această comandă, specificați calea completă a fișierului dumneavoastră .tar de dispozitiv virtual HMC.

6. În fișierul <XEN vHMC installation filename>.tar.gz este furnizat un fișier **vhmc.cfg**. Deschideți fișierul **vhmc.cfg** într-un editor de text și editați următoarele valori:
 - a. Schimbați numele consolei HMC virtuale (opțional): Editați fișierul **vhmc.cfg** și verificați că este corectă calea către discurile dumneavoastră. Fișierul conține șirul **DISK_PATH**.
 - b. Înlocuiți **DISK_PATH** cu calea pentru disk1.img:

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

- c. Înlocuiți **ethernet adapter** și adăugați adresa MAC (opțional):

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

Adresa opțională MAC:

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

Notă: Când este repornit Virtual HMC, hipervizorul Xen regenerează automat o adresă MAC. Adăugarea adresei MAC opționale rezolvă această problemă.

- d. Înlocuiți **FLOPPYPATH** (dacă folosiți Activation Engine):

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

7. Pentru a crea și porni VM, rulați comanda următoare: `xl create vHMC.cfg`.
8. Pentru a verifica dacă a fost adăugat VM-ul la lista de mașini virtuale definite, rulați comanda următoare: `xl list`.
9. Pentru a accesa consola locală VM, rulați comanda următoare: `vncviewer localhost 0`.

Instalarea unui dispozitiv virtual HMC folosind VMware ESXi

Aflați cum se instalează un dispozitiv virtual Hardware Management Console (HMC) folosind VMware ESXi.

Puteți instala un dispozitiv virtual HMC pe VMware ESXi folosind interfața grafică de utilizator pe clientul vSphere pentru a implementa șablonul Open Virtualization Format (OVF).

Notă: Puteți să instalați un dispozitiv virtual HMC pe VMware ESXi versiunea 6.0 sau ulterioară.

Pentru a instala un dispozitiv virtual HMC pe VMware ESXi folosind clientul vSphere, parcurgeți pașii următori:

Notă: Sintaxa comenzilor poate varia în funcție de sistemul de operare.

1. Obțineți fișierul arhivă tar: <nume fișier de instalare VMware vHMC>.tgz.
2. Folosiți comanda `tar` pentru a extrage fișierul OVA din fișierul arhivă tar.
3. Porniți clientul vSphere și logați-vă la gazda ESXi.
4. Din meniul **File**, selectați **Deploy OVF template**.
5. Faceți clic pe **Browse** și selectați fișierul OVA.
6. Faceți clic pe **Next**.

7. După finalizarea implementării, faceți clic pe **Close** și selectați pictograma de dispozitiv virtual HMC pentru a porni respectivul dispozitiv virtual HMC.

Instalarea unui dispozitiv virtual HMC pe POWER

Aflați cum să instalați un dispozitiv virtual Hardware Management Console (HMC) pe un mediu virtualizat POWER.

Instalarea unui dispozitiv virtual HMC pe PowerVM (partiție logică)

Aflați cum se instalează un dispozitiv virtual Hardware Management Console (HMC) într-un mediu PowerVM.

Un dispozitiv virtual HMC suportă servere POWER9 cu nivelul de firmware FW910 sau ulterior. Pentru informații suplimentare, consultați [Supported Linux distributions for POWER8 and POWER9 Linux on Power systems](https://www.ibm.com/support/knowledgecenter/en/linuxonibm/liaam/liaamdistros.htm) (<https://www.ibm.com/support/knowledgecenter/en/linuxonibm/liaam/liaamdistros.htm>).

Note:

1. Nu puteți gestiona serverul care găzduiește un dispozitiv virtual HMC.
2. Nu puteți gestiona serverul care găzduiește alt dispozitiv virtual HMC ce gestionează serverul ce găzduiește acest dispozitiv virtual HMC.

De exemplu, dispozitivul virtual HMC A rulează pe serverul A și dispozitivul virtual HMC B rulează pe serverul B. Dispozitivul virtual HMC A nu poate gestiona serverul B și dispozitivul virtual HMC B nu poate gestiona serverul A în același timp. Unul dintre dispozitivele virtuale HMC poate gestiona celălalt server, dar cele două dispozitive virtuale HMC nu se pot gestiona unul pe celălalt în același timp.

Crearea unei imagini pentru instalarea automată a consolei HMC (opțional)

Puteți crea o imagine pentru instalarea automată a consolei HMC care va instala automat un dispozitiv virtual HMC fără a afișa promptul pentru vrăjitorul **HMC Installation**.

Notă: Un dispozitiv virtual HMC pe PowerVM nu furnizează suport pentru adaptoarele grafice alocate partiției. Puteți utiliza un browser de web acceptat pentru a vă conecta la interfața de utilizator a consolei HMC.

Pentru a crea o imagine de instalare automată a consolei HMC, urmați pașii:

1. Creați două directoare rulând comenzile următoare: `mkdir -p oldiso` și `mkdir -p newiso`.
2. Montați imaginea de instalare HMC în directorul **oldiso** rulând următoarea comandă: `sudo mount -o loop <image_path> oldiso`.
3. Copiați conținutul directorului **oldiso** în directorul **newiso** rulând comanda: `cp -r oldiso/* newiso`.
4. Editați fișierul Grub pentru instalarea automată prin rularea comenzii următoare: `sed -i 's/biosdevname=0/biosdevname=0 mode=auto optype=Install/' newiso/boot/grub/grub.cfg`.
5. Faceți fișierul Grub cu drept doar pentru citire rulând următoarea comandă: `sudo chown 0444 newiso/boot/grub/grub.cfg`.
6. Creați un nou ISO pentru instalarea HMC rulând următoarea comandă: `mkisofs -o <new_iso_name> -V <ISO label> -f -r -T -udf --allow-limited-size --netatalk -chrip-boot -iso-level 4 -part -no-desktop -quiet newiso` (unde **ISO label** trebuie să fie HMC-<hmc version release number>, de exemplu HMC-8.0.870.0).

Notă: Pentru mai multe informații despre setarea Activation Engine și a fișierului de configurație, consultați [“Utilizarea Activation Engine pentru un dispozitiv virtual HMC”](#) la pagina 29.

Setarea volumului logic

Pentru a seta volumul logic, urmați pașii:

1. Selectați un sistem gestionat
2. Din blocul de meniuri, selectați **System Actions > Power VM > Virtual Storage**.
3. Selectați **Manage System VIOS > Action > Manage Virtual Storage**.
4. Selectați fila **Virtual Disks**.
5. Faceți clic pe **Create virtual disk** și introduceți următoarele informații:
 - **Virtual disk name:** Numele discului virtual.
 - **Storage pool name:** Numele pool-ului de stocare.
 - **Virtual disk size:** Dimensiunea discului virtual.
 - **Assigned partition:** Numele partiției logice.

Notă: Este necesar un spațiu de stocare pe disc de minim 160 GB (recomandat, 500 GB de spațiu pe disc).

Configurarea mediului de instalare - creare bibliotecă media

Pentru a crea o bibliotecă media, urmați pașii:

1. Selectați un sistem gestionat
2. Din blocul de meniuri, selectați **System Actions > Power VM > Virtual Storage**.
3. Selectați **Manage System VIOS > Action > Manage Virtual Storage**.
4. Selectați fila **Optical Devices**.
5. Faceți clic pe **Create Library** și introduceți următoarele informații:
 - **Storage pool:** Numele pool-ului de stocare.
 - **Media library size:** Dimensiunea bibliotecii media.
6. Faceți clic pe **OK**.

Configurarea mediului de instalare - Încărcare medii pe VIOS

Pentru a încărca medii pe Virtual I/O Server (VIOS), urmați pașii:

1. Conectați-vă la VIOS.
2. În modul VIOS, rulați comanda următoare: `oem_setup_env`.
3. Pentru a permite conexiunea NFS, rulați comanda următoare: `nfs -o nfs_use_reserved_ports=1`.
4. Pentru a monta NFS pe directorul local VIOS, rulați comanda: `mount <server_ip>:/Mountpoint <local_folder>`.
5. Pentru a verifica dacă montarea NFS include fișierul ISO de instalare HMC și imaginea de configurare Activation Engine (Opțional), rulați următoarea comandă: `ls`.

Configurarea mediului de instalare - Legare medii la biblioteca media

Pentru a lega medii la biblioteca de medii, urmați pașii:

1. Selectați **Manage System VIOS > Action > Manage Virtual Storage** și apoi selectați fila **Optical Devices**.
2. Din secțiunea **Virtual Optical Media** selectați **Add Media** din meniul **Actions**.
3. Din fereastra **Add Virtual Media** selectați **Add existing file from VIOS filesystem** și introduceți următoarele informații:
 - **Media name:** Numele mediului (de exemplu HMCInstall sau AEDrive).

- **Optical media file name:** Numele fișierului ISO de instalare (de exemplu, 01234567-ppc64ie.iso).
4. Faceți clic pe **OK**.
 5. Dacă ați creat o imagine de configurare Activation Engine, repetați pașii [3](#) - [4](#) pentru a adăuga imaginea de configurare Activation Engine. Altfel, continuați cu pasul [6](#).
 6. Verificați dacă mediul optic este încărcat în biblioteca media verificând dacă numele mediului este afișat în lista **Virtual Optical Media** disponibile.

Setarea partiției logice

Pentru a seta partiția logică, urmați pașii:

1. Selectați un sistem gestionat
2. Din blocul de meniuri, selectați **System Actions > Partitions > Partitions**.
3. Faceți clic pe **Create Partition** și introduceți informațiile următoare:
 - **Partition Name:** Numele partiției.
 - **Partition ID:** ID-ul partiției.
 - **Partition Type:** Selectați sistemul de operare (**AIX/Linux** sau **IBM i**).
4. Faceți clic pe **OK**.
5. Alocați numărul de procesoare și cantitatea de memorie pentru partiție.

Notă: Este necesar un minim de patru procesoare virtuale și 8 GB de memorie.
6. Din blocul de meniuri, selectați **Partition Actions > Virtual I/O > Virtual Networks**.
7. Faceți clic pe **Attach Virtual Network** și selectați caseta de bifare **Show and attach new virtual ethernet adapters**. Din tabel, selectați adaptoarele de rețea virtuală pe care vreți să le atașați partiției logice.

Notă: Sunt permise maximum patru adaptoare de rețea virtuală.
8. Din blocul de meniuri, selectați **Partition Actions > Virtual I/O > Virtual Storage**.
9. Din fila **Virtual Optical Device**, faceți clic pe **Add Virtual Optical Device**.
10. Introduceți **Device Name** (de exemplu, HMCInstall sau AEDrive) și apoi selectați din tabel serverul VIOS dorit.

Notă: Instalarea AEDrive este opțională.
11. Faceți clic pe **OK**.
12. Verificați dacă dispozitivele optice virtuale pe care le-ați adăugat la pasul [10](#) sunt listate în tabel.
13. Din meniul **Action**, faceți clic pe **Load**.
14. Selectați fișierul media de alocat la partiția logică și apoi apăsați **OK**.
15. Verificați dacă dispozitivele optice virtuale pe care le-ați încărcat la pasul [13](#) sunt listate în tabel.

Pornirea unui dispozitiv virtual HMC

Notă: Când instalați un dispozitiv virtual HMC pe o partiție folosind fișierul de imagine ISO HMC, nu veți avea acces cu consola grafică locală la interfața de utilizator web.

Pentru a porni un dispozitiv virtual HMC pe PowerVM, urmați pașii:

1. Selectați partiția gestionată.
2. Deschideți o conexiune activă la partiția logică selectând **Actions > Console > Open Terminal Window**.
3. Activați partiția logică selectând **Actions > Activate**.
4. Selectați **Activate (Normal)** și **Current Configuration**.

5. Faceți clic pe **Finish**.
6. Comutați la fereastra terminal.
7. Din meniul **Boot**, selectați **1 = SMS Menu**.
8. Din meniul **Main**, selectați **5 = Select Boot Options**.
9. Din meniul **Multiboot**, selectați **1 = Select Install/Boot Device**.
10. Din meniul **Select Device Type**, selectați **5 = List all devices**.
11. Selectați dispozitivul HMCInstall pe baza locației dispozitivului.
12. Selectați **2. Normal Mode Boot**.
13. Selectați **1. Yes** pentru a confirma.
14. Urmați instrucțiunile afișate de vrăjitorul **HMC Install**.

Notă: Săriți acest pas dacă ați folosit o imagine de instalare automată a consolei HMC.

15. După ce instalarea se termină și sistemul pornește, trebuie să selectați o limbă din caseta de dialog **language selection**.
16. Acceptați acordul de licență.

Notă: Asigurați-vă că controlerul de comenzi este gata să accepte comenzi înainte de a rula orice comandă. De exemplu, rulând comanda **lshmc -V** până când reușește.

17. Logați-vă ca hscroot și folosiți comanda **chhmc** pentru a configura rețeaua.

Următorul exemplu arată secvența comenzilor **chhmc** care pot fi folosite pentru a configura rețeaua și a activa SSH (Secure Shell) și accesul web la distanță pe HMC.

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

- **ethX** este numele interfeței de rețea ce trebuie configurat.
- **hmc ip address** este adresa IP a consolei dumneavoastră HMC.
- **hmc network mask** este masca de rețea a consolei dumneavoastră HMC.
- **hmc hostname** este numele de gazdă al consolei dumneavoastră HMC.
- **hmc domain name** este numele de domeniu al consolei dumneavoastră HMC.
- **gateway ip** este adresa IP a gateway-ului pe rețeaua dumneavoastră.
- **name server** este numele adresei de server al rețelei dumneavoastră.
- **domain search** reprezintă numele domeniilor în care doriți să caute consola HMC.
- Pentru a permite accesul pe toate adresele IP, folosiți **-a 0.0.0.0 -nm 0** în loc de **ip address**.

Notă: Când utilizați mai multe adaptoare Ethernet virtuale, rulați comanda **cat /etc/sysconfig/network-scripts/ifcfg-ethX** pentru dispozitiv virtual HMC pe fiecare interfață. Comparați adresa MAC (Media Access Control) cu ce afișează consola HMC în vizualizarea de adaptor al rețelei virtuale a partiției. Puteți apăsa pe **View Virtual Ethernet Adapter Settings** pentru mai multe informații despre adaptoarele Ethernet virtuale. Acest pas vă ajută să determinați interfața corectă pentru utilizare.

18. Reporniți sistemul.

Utilizarea Activation Engine pentru un dispozitiv virtual HMC

Aflați cum se utilizează Activation Engine pentru un dispozitiv virtual Hardware Management Console (HMC).

Activation Engine este un cadru de lucru care permite diferitelor componente dintr-o mașină virtuală să fie configurate în timpul pornirii sistemului. Pentru a utiliza Activation Engine, trebuie să setați un profil de configurare XML pentru a permite ca un dispozitiv virtual HMC să fie într-o stare gata-de-gestionare la prima pornire. Pentru informații suplimentare despre configurarea profilului de configurare XML, vedeți [“Setarea profilului de configurare pentru Activation Engine” la pagina 30](#). Fișierul de configurație poate fi folosit pentru a configura opțiunile următoare:

- Setarea tastaturii implicite (US)
- Locale-ul implicit (US)
- Dezactivarea setărilor tastaturii
- Dezactivarea setărilor ecranului
- Acordul de licență și Acord codului de mașină
- Dezactivarea vrăjitor de setare
- Dezactivarea vrăjitorului call-home
- Configurarea a până la patru plăci NIC (Network Interface Card)
- Configurarea setărilor de firewall pentru fiecare interfață
- Configurarea interfeței rețelei ca server DHCP pentru IPv4
- Configurarea interfeței Private și Open
- Configurarea dispozitivului de interfață gateway implicit

Notă: Numărul de adaptoare Ethernet care este definit în fișierul de configurație **vHMC-Conf.xml** trebuie să corespundă cu adaptoarele de rețea definite în fișierele de configurație **domain.xml**, **vHMC.cfg** sau **VMWare**.

Activation Engine necesită un disc virtual care să rețină o configurație XML. Puteți edita fișierul **user_data** cu un editor de text și să folosiți ghidul pentru configurația XML care este afișat în exemplul următor.

Pentru a crea un disc cu imaginea virtuală ISO a configurației Activation Engine într-un mediu Linux urmați pașii:

1. Creați un director:

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

2. Copiați fișierul editat **user_data** în directorul:

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

3. Creați o imagine de disc virtuală a configurației Activation Engine:

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

Setarea profilului de configurare pentru Activation Engine

Învățați cum să setați fișierul de configurație Activation Engine prin folosirea tagurilor XML.

Fișierul de configurație

Folosiți următorul exemplu de fișier de configurație pentru a învăța despre tagurile XML.

```
<vHMC-Configuration>
  <ConfigurationVersion>2.0</ConfigurationVersion>
  <LicenseAgreement></LicenseAgreement>
  <AcceptLicense>Yes</AcceptLicense>
  <Locale>en_US.UTF-8</Locale>
  <SetupWizard>No</SetupWizard>
  <SetupCallHomeWizard>No</SetupCallHomeWizard>
  <SetupKeyboard>No</SetupKeyboard>
  <SetupDisplay>No</SetupDisplay>
  <Ethernet Enable='Yes' DefaultGatewayDevice='Yes' PrivateInterface='No'>
    <Hostname></Hostname>
```

```

<Domain></Domain>
<DNSServers></DNSServers>
<IPV4Config>
  <NetworkType></NetworkType>
  <IPAddress></IPAddress>
  <Netmask></Netmask>
  <Gateway></Gateway>
</IPV4Config>
<IPV6Config>
  <NetworkType></NetworkType>
  <IPAddress></IPAddress>
  <Gateway></Gateway>
<IPV6Config>
<Firewall>
  <PEGASUS>Enabled</PEGASUS>
  <RPD>Enabled</RPD>
  <FCS>Enabled</FCS>
  <I5250>Enabled</I5250>
  <PING>Enabled</PING>
  <L2TP>Disabled</L2TP>
  <SLP>Enabled</SLP>
  <RSCT>Enabled</RSCT>
  <SECUREREMOTEACCESS>Enabled</SECUREREMOTEACCESS>
  <SSH>Enabled</SSH>
  <NTP>Disabled</NTP>
  <SNMPTraps>Disabled</SNMPTraps>
  <SNMPAgents>Disabled</SNMPAgents>
</Firewall>
</Ethernet>
<NTPServers>
  <ntpparam ntpserver="" ntpversion=""/>
</NTPServers>
</vHMC-Configuration>

```

Tagurile XML pentru fișierul de configurație

Tagurile XML sunt folosite în fișierul de configurație Activation Engine pentru a seta valorile specifice pentru diferite atribute. Puteți să setați manual aceste valori în fișierul de configurație Activation Engine. Folosiți tabelul următor pentru a vedea o descriere a fiecărui tag și valorile sale permise:

Tabela 9. Taguri XML			
Taguri	Descriere	Valori acceptabile	Note
ConfigurationVersion	Element necesar care definește versiunea de configurare pentru utilizare.	2.0	
LicenseAgreement	Element necesar care afișează Acordul de licență pentru dispozitiv virtual HMC.		
AcceptLicense	Element necesar pentru a accepta Acordul de licență pentru dispozitiv virtual HMC.	Yes: Acceptă Acordul de licență HMC. No: Se afișează un prompt care invită utilizatorul să accepte Acordul de licență HMC	Dacă este introdusă o valoare invalidă, Activation Engine folosește setarea implicită No .
Locale	Element necesar pentru definirea setărilor de Locale.	en_US.UTF-8	Dacă este introdusă o valoare invalidă, Activation Engine folosește valoarea implicită US .

Tabela 9. Taguri XML (continuare)

Taguri	Descriere	Valori acceptabile	Note
SetupWizard	Element necesar pentru a activa sau dezactiva vrăjitorul HMC Setup .	Yes: Afișează vrăjitorul HMC Setup. No: Dezactivează afișarea vrăjitorului HMC Setup.	Dacă este introdusă o valoare invalidă, Activation Engine folosește valoarea implicită Yes .
SetupCallHomeWizard	Element necesar pentru a activa sau dezactiva vrăjitorul HMC Call Home .	Yes: Afișează vrăjitorul HMC Call Home. No: Dezactivează afișarea vrăjitorului HMC Call Home.	Dacă este introdusă o valoare invalidă, Activation Engine folosește valoarea implicită Yes .
SetupKeyboard	Element necesar pentru a defini configurarea tastaturii.	Yes: Invită utilizatorul cu un prompt la configurarea tastaturii. No: Acceptă configurația implicită a tastaturii (US).	Dacă este introdusă o valoare invalidă, Activation Engine folosește valoarea implicită Yes .
SetupDisplay	Element necesar pentru a activa sau dezactiva configurarea ecranului.	Yes: Invită utilizatorul cu un prompt la configurarea ecranului. No: Acceptă configurarea implicită a ecranului.	Dacă este introdusă o valoare invalidă, Activation Engine folosește valoarea implicită Yes .
Ethernet	Element necesar care păstrează valorile pentru configurările adaptorului Ethernet. Pot fi configurate maxim patru adaptoare Ethernet.	Enable: Yes: Configurați acest adaptor. No: Nu configurați acest adaptor. DefaultGatewayDevice: Yes: Configurați acest adaptor ca adaptor de rețea principal. No: Nu configurați acest adaptor ca adaptor de rețea principal. PrivateInterface: Yes: Configurați acest adaptor ca interfață privată. Yes este necesar pentru a configura interfața ca server DHCP IPv4. No: Nu configurați acest adaptor ca interfață privată. No este necesar pentru a configura interfața de tip IPv4 static.	Activation Engine rulează configurația implicită dacă sunt introduse valori invalide în secțiunea adaptorului Ethernet sau dacă sunt definite mai multe Default Gateway Devices . Elementele opționale pot fi omise la configurare. Este necesară cel puțin o configurație IPV4 sau IPV6. Dacă nu specificați nici o configurație IP, Activation Engine va folosi configurația implicită.
HostName	Element opțional pentru a defini numele de gazdă rețea.	Orice șir valid pentru numele de gazdă.	Dacă elementul nu este definit, Activation Engine folosește valoarea implicită a gazdei locale HostName .

Tabela 9. Taguri XML (continuare)

Taguri	Descriere	Valori acceptabile	Note
Domain	Element opțional pentru a defini domeniul de rețea.	Orice valoare validă a domeniului (de exemplu, example.us.com).	Dacă elementul nu este definit, Activation Engine folosește valoarea implicită Domain goală.
DNSServers	Element opțional pentru a defini serverele de rețea DNS.	Este acceptabil să aveți o valoare validă a serverului DNS sau până la trei adrese IPv4 sau IPv6 valide care sunt separate prin virgulă. - Exemplul 1: IPv4: 8.3.2.1 IPv6: 2001:4860:4860::8888 - Exemplul 2: IPv4: 8.3.2.1,8.5.4.1 IPv6: 2001:4860:4860::8888,2001:4860:4860::8844 - Exemplul 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	Dacă elementul nu este definit, Activation Engine folosește valoarea implicită DNSServers goală.
IP4Config	Element opțional pentru a defini setările configurației IPv4.	IPType: Element necesar pentru a defini tipul configurației IPv4. Static: Configurați acest adaptor folosind configurarea statică. DHCP: Configurați acest adaptor folosind configurarea DHCP. DHCPServer: Configurați acest adaptor ca server DHCP IPv4 (necesită ca PrivateInterface să fie setat la Yes). IPAddress: Element opțional care este necesar doar dacă este selectată configurația Static sau DHCPServer. Static Configuration: Orice valoare validă a adresei IPv4. DHCPServer Configuration: Orice IP de server DHCP din intervalul de IP-uri. Netmask: Element opțional care este necesar doar dacă este selectată configurația Static. - Orice valoare validă de mască de rețea IPv4. Gateway: Element opțional care este necesar doar dacă este selectată configurația Static. - Orice valoare validă a măștii de rețea IPv4.	

Tabela 9. Taguri XML (continuare)

Taguri	Descriere	Valori acceptabile	Note
IP6Config	Element opțional pentru a defini setările configurației IPv6.	IPType: Element necesar pentru a defini tipul configurației IPv6. • Static: Configurați acest adaptor folosind configurarea statică. • DHCP: Configurați acest adaptor folosind configurarea DHCP. IPAddress: Este acceptabil să existe o formă lungă sau scurtă de format IPv6 și o formă lungă sau scurtă de prefix IPv6. • Exemplul 1: IPv6: 2001:4860:4860:0000:0000:0000:8888 • Exemplul 2: IPv6: 2001:4860:4860::8888 • Exemplul 3: IPv6: 2001:4860:4860::8888/128 Dacă nu este specificat un prefix, Activation Engine utilizează setarea implicită a prefixului, /64. Gateway: • Orice valoare validă de adresă IPv6.	

Tabela 9. Taguri XML (continuare)

Taguri	Descriere	Valori acceptabile	Note
Firewall	Element opțional pentru a defini setările firewall-ului.	PEGASUS: • Enabled: Permite porturilor PEGASUS să fie deschise. • Disabled: Dezactivează porturile PEGASUS. RPD: • Enabled: Permite porturilor RMC să fie deschise. • Disabled: Dezactivează porturile RMC. FCS: • Enabled: Permite porturilor FCS să fie deschise. • Disabled: Dezactivează porturile FCS. I5250: • Enabled: Permite porturilor 5250 să fie deschise. • Disabled: Dezactivează porturile 5250. PING: • Enabled: Permite portului Ping să fie deschis. • Disabled: Dezactivează portul Ping. L2TP: • Enabled: Permite porturilor L2TP să fie deschise. • Disabled: Dezactivează porturile L2TP. SLP: • Enabled: Permite porturilor SLP să fie deschise. • Disabled: Dezactivează porturile SLP. RSCT: • Enabled: Permite porturilor RSCT să fie deschise. • Disabled: Dezactivează porturile RSCT. SECUREREMOTEACCESS: • Enabled: Permite porturilor securizate de acces la distanță să fie deschise. • Disabled: Dezactivează porturile securizate de acces la distanță. SSH: • Enabled: Permite portului SSH să fie deschis. • Disabled: Dezactivează portul SSH.	

Tabela 9. Taguri XML (continuare)			
Taguri	Descriere	Valori acceptabile	Note
Firewall	Element opțional pentru a defini setările firewall-ului.	NTP: • Enabled: Permite porturilor NTP să fie deschise. • Disabled: Dezactivează porturile NTP. SNMPTraps: • Enabled: Permite porturilor capcanelor SNMP să fie deschise. • Disabled: Dezactivează porturile capcanelor SNMP. SNMPAgents: • Enabled: Permite porturilor agenților SNMP să fie deschise. • Disabled: Dezactivează porturile agenților SNMP.	
NTPServers	Tagul NTPServers este necesar dacă doriți să configurați până la cinci servere NTP într-un dispozitiv virtual HMC.	NTPServers: Acceptă <ntpparam ntpserver="server" ntpversion="version"/> ntpparam: • ntpserver: Acceptă orice valori IPv4 sau IPv6 valide sau nume de gazdă valide. • ntpversion: Acceptă 1-4 valori numerice Exemplu: <pre><NTPServers> <ntpparam ntpserver="test.austin.ibm.com" ntpversion="2"/> <ntpparam ntpserver="192.168.34.1" ntpversion="4"/> <ntpparam ntpserver="::ffff:903:201" ntpversion="3"/> </NTPServers></pre>	

Configurarea consolei HMC

Aflați cum să setați conexiunile de rețea, să configurați consola HMC, să realizați pașii postconfigurare și să actualizați și modernizați consola HMC.

Alegerea setărilor de rețea pe HMC

Aflați despre setările de rețea pe care le puteți folosi pe consola HMC.

Conexiunile de rețea HMC

Aflați cum poate fi folosită consola Hardware Management Console HMC într-o rețea.

Puteți folosi diferite tipuri de conexiuni de rețea pe pentru a vă conecta consola HMC la sistemele gestionate. Pentru informații suplimentare despre cum să configurați HMC pentru conectare la o rețea, consultați “Configurarea consolei HMC” la [pagina 53](#). Pentru informații suplimentare despre utilizarea consolei HMC într-o rețea, vedeți următoarele:

Tipurile de conexiuni de rețea HMC

Aflați cum se utilizează gestionarea la distanță HMC și funcțiile de servicii utilizând rețeaua dumneavoastră.

Consola HMC suportă următoarele tipuri de comunicații logice:

HMC la sistemul gestionat

Folosită pentru a gestiona majoritatea funcțiilor de gestiune hardware, în care HMC emite cereri de funcții de control prin procesorul de service al sistemului gestionat. Conexiunea din consola HMC și procesorul de service este uneori cunoscută ca *rețea de service*. Această conexiune este necesară pentru gestiunea sistemelor gestionate.

HMC la partiția logică

Utilizat pentru a colecta informații legate de platformă (evenimente de erori de hardware, inventar hardware) de la sistemul de operare care rulează pe partițiile logice și, pentru a coordona anumite activități ale platformei (LPAR dinamic, reparare concomitentă) cu acele sisteme de operare. Dacă vreți să folosiți caracteristicile de notificare de service și eroare, trebuie să creați această conexiune.

HMC la BMC

Notă: Conexiunea BMC (baseboard management controller) este aplicabilă numai pentru modelul HMC 7063-CR1.

Folosită pentru a realiza taskuri de service și întreținere. Conexiunea BMC este folosită pentru a încărca și întreține firmware-ul HMC pe sistem. Această conexiune este necesară pentru accesul la BMC pe HMC.

HMC la utilizatorii de la distanță

Furnizează utilizatorilor la distanță acces la funcțiile HMC. Utilizatorii de la distanță pot accesa consola HMC în următoarele moduri:

- Utilizând browser-ul web pentru a accesa toate funcțiile GUI HMC la distanță.
- Utilizând Secure Socket Shell (SSH) pentru a accesa funcțiile de linie de comandă HMC la distanță.
- Utilizând un server terminal virtual pentru acces la distanță la console de partiții logice virtuale.

HMC la organizația de service și suport

Folosită pentru a transmite date, cum ar fi rapoarte de erori hardware, date de inventar și actualizări de microcod, de la și la furnizorul de service. Puteți folosi aceste căi de comunicații pentru a face apeluri automate la service.

Consola HMC acceptă până la patru interfețe Ethernet fizice separate, în funcție de model. Versiunea autonomă de HMC suportă numai trei interfețe HMC, prin utilizarea unui adaptor Ethernet integrat și maxim două adaptoare plug-in. Folosiți fiecare dintre aceste interfețe în următoarele moduri:

- O interfață de rețea poate fi folosită exclusiv pentru comunicațiile consolei HMC cu sistemul gestionat, ceea ce înseamnă că în rețea se vor afla doar consola HMC și procesoarele de service ale sistemelor gestionate. Una sau mai multe interfețe de rețea pot fi folosite exclusiv pentru comunicațiile consolei HMC cu sistemul gestionat, ceea ce înseamnă că doar HMC și procesoarele de service ale sistemelor gestionate se află în acea rețea. Chiar dacă interfețele de rețea către procesoarele de service sunt criptate pentru protocolul SSL (Secure Sockets Layer) și protejate prin parolă, existența unei rețele dedicate separate poate asigura un nivel mai înalt de securitate pentru aceste interfețe.
- De obicei, o interfață de rețea deschisă este folosită pentru conexiunea prin rețea între HMC și partițiile logice de pe sistemele gestionate, pentru comunicațiile consolei HMC cu partiția logică. Puteți de asemenea folosi această interfață de rețea deschisă pentru a gestiona consola HMC de la distanță.
- Opțional, puteți folosi o a treia interfață pentru conectarea la partiții logice și gestionarea consolei HMC de la distanță. Această interfață poate fi de asemenea folosită ca o conexiune separată HMC la grupuri diferite sau partiții logice. De exemplu, puteți dori să aveți o rețea locală administrativă care este separată de rețeaua locală pe care se derulează tranzacțiile activității uzuale. Administratorii la distanță pot accesa HMC și alte unități gestionate folosind această metodă. Uneori partițiile logice sunt în domenii diferite de securitate de Rețea, probabil în spatele unui firewall și puteți dori să aveți conexiuni diferite de rețea HMC în fiecare din acele două domenii.

Cerințele de browser web pentru HMC

Consola HMC (Hardware Management Console) versiunea 9.1.0 este suportată de Google Chrome versiunea 57, Microsoft Internet Explorer (IE) versiunea 11.0, Mozilla Firefox versiunile 45 și 52 Extended Support Release (ESR) și Safari versiunea 10.1.

Dacă browser-ul dumneavoastră este configurat pentru a utiliza un proxy de Internet, în lista de excepții trebuie să fie inclusă o adresă IP locală. Consultați administratorul dumneavoastră de rețea pentru informații suplimentare despre lista de excepții. Dacă trebuie încă să utilizați proxy-ul pentru a ajunge la HMC, activați Se utilizează HTTP 1.1 cu conexiunile prin proxy sub fila Complex din fereastra dumneavoastră Opțiuni Internet.

Cookie-urile de sesiune trebuie să fie activate pentru ca ASMI să funcționeze când este conectat la HMC de la distanță. Codul proxy asm salvează informații de sesiune și le utilizează. Urmați pașii pentru a activa cookie-urile de sesiune.

Activarea cookie-urilor de sesiune în Internet Explorer.

1. Selectați Unelte și faceți clic pe Opțiuni internet
2. Selectați Confidențialitate și faceți clic pe Avansat
3. Asigurați-vă că este bifată opțiunea Permite cookie-uri de sesiune întotdeauna. Dacă nu este, selectați Ignorare gestiune automată a modulelor cookie și selectați Întotdeauna se acceptă module cookie de sesiune.
4. Selectați Se solicită sub Module cookie originale și Module cookie de la terți.
5. Faceți clic pe OK.

Activarea cookie-urilor de sesiune în Firefox.

1. Selectați Unelte și faceți clic pe Opțiuni
2. Faceți clic pe Cookie-uri
3. Selectați Permiteți site-urilor să seteze cookie-uri.
4. Selectați Excepții și adăugați HMC.
5. Faceți clic pe OK.

Rețele private și deschise în mediul de lucru al consolei HMC

Consola HMC poate fi configurată să folosească rețele deschise și private. Rețelele private permit folosirea unui interval selectat de adrese IP nerutabile. O rețea *publică*, sau "deschisă", este conexiunea prin rețea a consolei HMC la partițiile logice, precum și la celelalte sisteme din rețeaua obișnuită.

Rețelele private

Singurele dispozitive dintr-o rețea privată HMC sunt consola HMC propriu-zisă și sistemele gestionate la care este conectată consola HMC. Consola HMC este conectată la FSP-ul (Flexible Service Processor) fiecărui sistem gestionat.

Pe majoritatea sistemelor, FSP asigură două porturi Ethernet, etichetate **HMC1** și **HMC2**. Aceasta vă permite să conectați până la două console HMC.

Unele sisteme au opțiunea unui FSP dual. În această situație, al doilea FSP acționează ca rezervă "redundantă". Cerințele setării de bază pentru un sistem cu două FSP-uri sunt în esență identice cu cele ale sistemelor care nu au al doilea FSP. Consola HMC trebuie conectată la fiecare FSP, deci este necesar hardware de rețea suplimentar (de exemplu, un switch sau hub LAN) unde există mai multe FSP-uri sau există mai multe sisteme gestionate.

Notă: Fiecare port FSP de pe sistemul gestionat trebuie să fie conectat la o singură consolă HMC.

Rețelele publice

Rețeaua deschisă poate fi conectată la un firewall sau ruter pentru conectarea la internet. Conectarea la internet permite consolei HMC să execute "call home" când există erori hardware care trebuie raportate.

Consola HMC asigură propriul firewall pentru fiecare interfață de rețea. Când rulați vrăjitorul HMC Guided Setup este configurat automat un firewall de bază, dar vă puteți personaliza setările pentru firewall după instalarea și configurarea inițială a consolei HMC.

HMC ca un server DHCP

Puteți utiliza consola (HMC) ca server DHCP (Dynamic Host Configuration Protocol).

Dacă doriți să configurați prima interfață a rețelei ca o rețea privată, puteți selecta dintr-un interval adresele IP pe care serverul DHCP urmează să le aloce clienților săi. Intervalele de adrese ce pot fi selectate includ segmente din intervalele standard de adrese IP nerutabile.

În plus față de aceste intervale standard, un interval special de adrese IP este rezervat pentru adresele IP. Acest interval special poate fi utilizat pentru a evita conflictele în cazuri în care rețelele deschise atașate HMC folosesc unul dintre intervalele de adrese nerutabile. Pe baza intervalului selectat, pentru interfața de rețea a consolei HMC dintr-o rețea privată este alocată automat prima adresă IP din acel interval, iar pentru procesoarele de service sunt alocate restul adreselor din interval.

Serverul DHCP din consola HMC folosește alocarea automată, ceea ce înseamnă că fiecărei interfețe Ethernet unice a procesorului de service îi este realocată aceeași adresă IP de fiecare dată când este pornită. Fiecare interfață Ethernet are un identificator unic care se bazează pe o adresă MAC (Media Access Control) încorporată, care permite serverului DHCP să realocheze aceiași parametri IP. Puteți configura ambele porturi HMC **eth0** și **eth1** HMC pentru a servi adrese DHCP. Puteți configura ambele porturi HMC **eth0** și **eth1** HMC pentru a servi adrese DHCP.

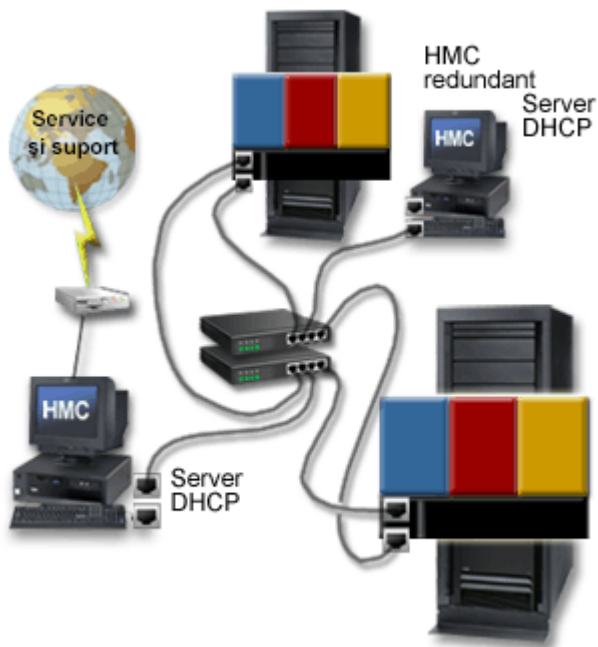
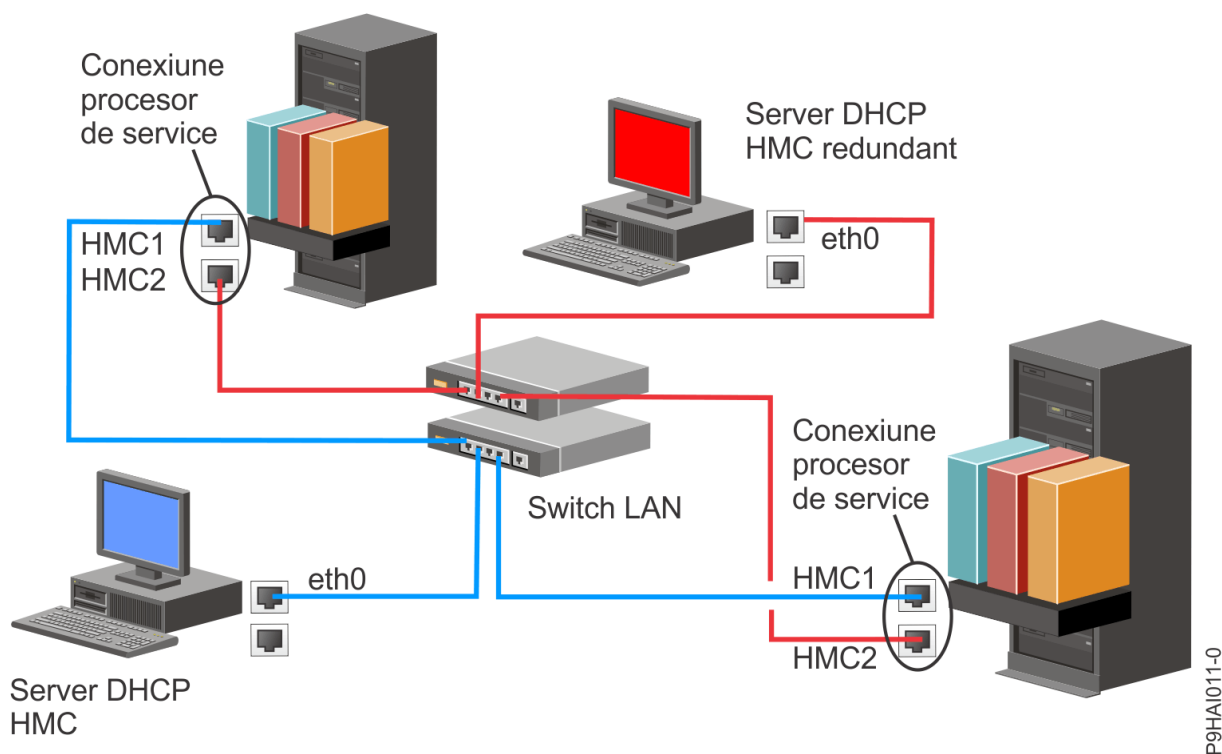


Figura 9. Rețea privată cu o consolă HMC ca server DHCP

Notă: Dacă folosiți IPv6, procesul de descoperire trebuie să fie realizat manual. Pentru IPv6, nu există descoperire automată.

Pentru informații suplimentare despre configurarea consolei HMC ca un server DHCP, vedeți ["Configurarea consolei HMC ca server DHCP"](#) la pagina 61.

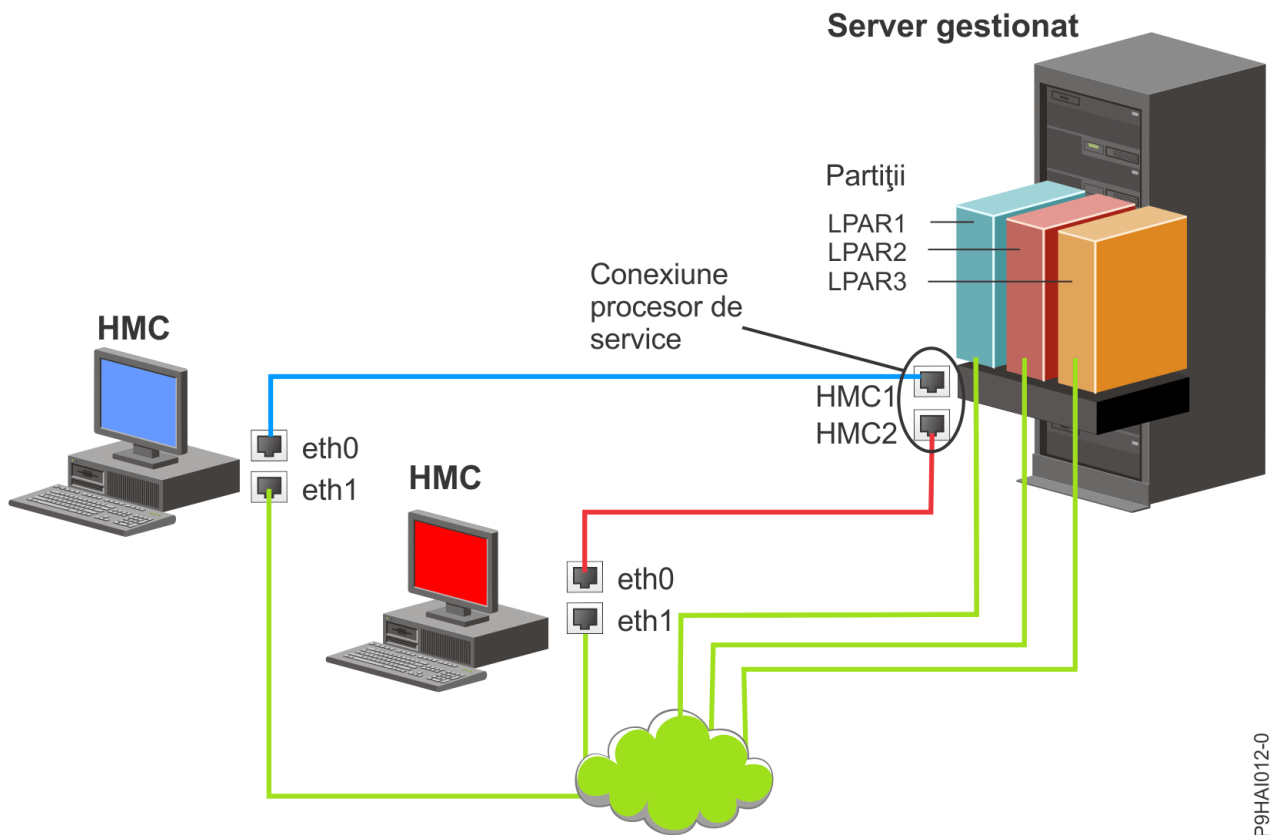


Această ilustrație prezintă un mediu de lucru cu consolă HMC redundantă și două sisteme gestionate. Prima consolă HMC este conectată la primul port al fiecărui FSP, iar consola HMC redundantă este conectată la al doilea port al fiecărui FSP. Fiecare consolă HMC este configurată ca server DHCP, folosind un interval diferit de adrese IP. Conexiunile sunt în rețele private separate. Ca urmare, este important să vă asigurați că niciun port FSP nu este conectat la mai mult de o consolă HMC.

Fiecare port FSP al sistemului gestionat care este conectat la o consolă HMC necesită o adresă IP unică. Pentru a vă asigura că fiecare port FSP are o adresă IP unică, folosiți capacitatea de server DHCP încorporată în HMC. Când FSP detectează legătura activă la rețea, lansează o cerere broadcast pentru localizarea unui server DHCP. Când este configurată corect, consola HMC răspunde acestei cereri prin alocarea uneia dintre adresele intervalului selectat.

Dacă aveți mai multe FSP-uri, trebuie să aveți propriul switch sau hub LAN pentru consola HMC la rețeaua privată FSP. Sau acest segment privat poate exista ca un grup de câteva porturi într-un *LAN virtual* (VLAN) privat al unui switch gestionat mai mare. Dacă aveți mai multe VLAN-uri private, trebuie să vă asigurați că sunt izolate și că nu există trafic între ele.

Dacă aveți mai multe console HMC, trebuie de asemenea să conectați fiecare consolă HMC cu celelalte și la partițiile logice, în aceeași rețea deschisă.



Această figură arată două console HMC conectate la un singur server gestionat în rețeaua privată și la trei partiții logice în rețeaua publică. Puteți avea un adaptor Ethernet adițional pentru consola HMC, pentru a avea trei interfețe de rețea. Puteți să folosiți a treia rețea ca o rețea de gestionare sau să o conectați la CSM (Cluster Systems Manager) Management Server.

Alegerea metodei de conectivitate care va fi folosită pentru serverul call-home

Aflați mai multe despre opțiunile de conectivitate pe care le aveți atunci când folosiți serverul call-home.

Puteți configura consola HMC să trimită informații legate de service hardware către IBM folosind o conexiune la Internet bazată pe LAN sau la o conexiune dial-up peste un modem.

Aveți două alegeri de comunicație când configurați conexiunea la Internet bazată pe LAN. Prima opțiune este să folosiți SSL (Secure Sockets Layer) standard. Puteți activa comunicația SSL pentru conectarea la Internet printr-un server proxy. Cu conectivitatea SSL este mai probabil să fie respectate indicațiile privind securitatea în întreprindere.

Notă: În cazul în care conexiunea interfeței dumneavoastră de rețea deschisă folosește doar Internet Protocol Versiunea 6 (IPv6), nu puteți folosi Internet VPN pentru a vă conecta la suport. Pentru informații suplimentare despre protocoalele utilizate, vedeți [“Alegerea unui protocol IP” la pagina 43](#).

Printre avantajele folosirii unei conexiuni Internet se numără:

- Viteză de transmisie mai mare
- Costuri de beneficiar reduse (de exemplu, costul unei linii telefonice analogice dedicate)
- Fiabilitate mai mare

Sunt valabile următoarele caracteristici de securitate, indiferent de metoda de conectivitate aleasă:

- Cererile Remote Support Facility sunt întotdeauna inițiate din HMC către IBM. O conexiune de intrare nu este niciodată inițiată de la sistemul IBM Service Support.
- Toate datele care sunt transferate între HMC și IBM Service Support System sunt cifrate folosind o cifrare de nivel înalt. Funcție de metoda de conectivitate aleasă, datele sunt cifrate folosind fie SSL, fie IPsec ESP (Encapsulating Security Payload).

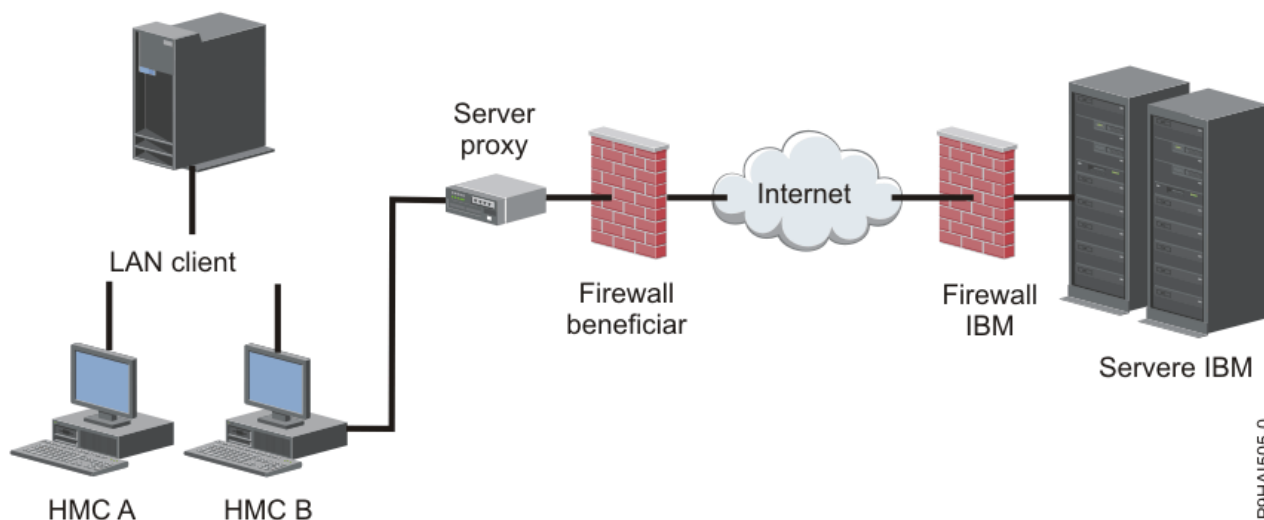
- Când inițializați conexiunea criptată, HMC autentifică destinația țintă ca fiind cea a IBM Service Support System.

Datele trimise la sistemul IBM Service Support sunt numai informații referitoare la configurația și problemele hardware-ului. Nu este transmisă nicio aplicație și nici date de client către IBM.

Folosirea unei conexiuni Internet indirecte cu un server proxy

Dacă instalarea cere ca HMC să fie pe o rețea privată, este posibil să vă conectați indirect la Internet folosind un proxy SSL, care poate înainta cererile către Internet. Unul dintre celelalte avantaje potențiale ale utilizării unui proxy SSL este că proxy-ul poate suporta facilități de jurnalizare și de auditare.

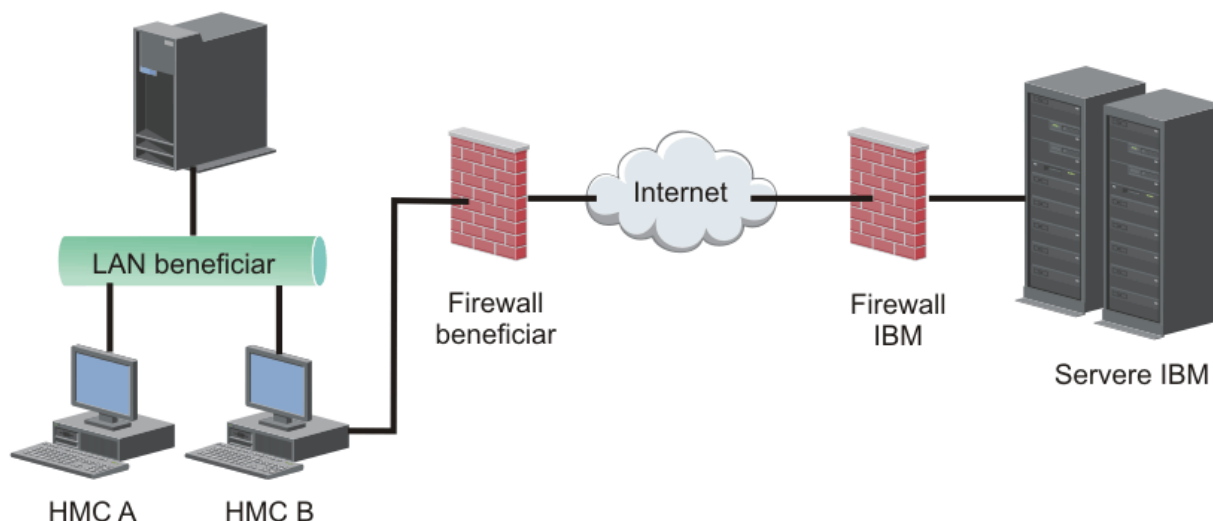
Pentru a înainta socket-uri SSL, serverul proxy trebuie să suporte funcțiile de antet proxy de bază (așa cum se specifică în RFC 2616) și metoda CONNECT. Opțional, autentificarea proxy de bază (RFC 2617) poate fi configurată astfel încât HMC să se autentifice înainte de a încerca să înainteze socketuri prin intermediul serverului proxy.



Pentru ca HMC să reușească intrarea în comunicare, serverul proxy al clientului trebuie să permită conexiuni la portul 443. Vă puteți configura serverul proxy astfel încât să limiteze adresele IP specifice la care se poate conecta HMC. Vedeți [“Listele cu adrese Internet SSL”](#) la [pagina 43](#) pentru o listă cu adresele IP.

Folosirea conexiunii Internet directe SSL

În cazul în care consola dumneavoastră HMC poate fi conectată la Internet și firewall-ul extern poate fi setat astfel încât să permită circulația pachetelor TCP stabilite în exterior, către destinațiile menționate în [“Listele cu adrese Internet SSL”](#) la [pagina 43](#) puteți folosi o conexiune Internet directă.



P9HAI504-0

Folosirea unei conexiuni Internet SSL pentru conectarea la organizația de suport de la distanță

Toate comunicațiile sunt tratate prin socket-uri TCP inițiate de HMC și folosesc SSL de nivel înalt pentru criptarea datelor transmise. Adresele TCP/IP destinație sunt publicate (vedeți [“Listele cu adrese Internet SSL”](#) la pagina 43), astfel că firewall-urile externe pot fi configurate pentru a permite aceste conexiuni.

Notă: Pentru toate comunicațiile este folosit portul 443 HTTPS standard.

Consola HMC poate fi activată pentru conectare directă la Internet sau pentru conectare indirectă, de pe un server proxy furnizat de beneficiar. Alegerea celei mai bune abordări pentru instalarea dumneavoastră depinde de cerințele de securitate și de rețea în întreprinderea dumneavoastră. Consola HMC (conectată direct sau prin proxy-ul SSL) folosește următoarele adrese când este configurată să utilizeze conectivitatea Internet SSL.

Alegerea unui protocol IP

Determinați versiunea de adresă IP folosită când consola HMC se conectează la furnizorul de servicii.

Majoritatea utilizatorilor folosesc Internet Protocol Versiunea 4 (IPv4) pentru a se conecta la furnizorul de servicii. Adresele IPv4 apar în formatul ce reprezintă cei patru octeți separați prin puncte ai adresei IPv4 (de exemplu 9.60.12.123) pentru accesul la Internet. Puteți folosi și Internet Protocol Versiunea 6 (IPv6) pentru a vă conecta la furnizorul de servicii. IPv6 este folosit adesea de administratorii de rețea pentru a asigura un spațiu de adrese unic. Dacă nu sunteți sigur ce protocol IP este utilizat în instalarea dumneavoastră, contactați administratorul de rețea. Pentru informații suplimentare despre folosirea fiecărei versiuni, vedeți [“Setarea adresei IPv4”](#) la pagina 62 și [“Setarea adresei IPv6”](#) la pagina 62.

Listele cu adrese Internet SSL

Vedeți ce adrese folosește consola HMC (Hardware Management Console) atunci când utilizează conectivitatea Internet SSL.

Consola HMC folosește adresele IPv4 următoare pentru a contacta serviciul și suportul IBM când este configurat pentru folosirea conectivității Internet SSL.

Următoarele adrese IPv4 sunt pentru toate locațiile:

- 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

Următoarele adrese IPv4 sunt pentru America:

- 129.42.160.48
- 129.42.160.49
- 207.25.252.197
- 207.25.252.200
- 207.25.252.204

Următoarele adrese IPv4 sunt pentru toate locațiile în afara Americilor:

- 129.42.160.48
- 129.42.160.50
- 207.25.252.197
- 207.25.252.200
- 207.25.252.205

Notă: Când se configurează un firewall pentru a permite consolei HMC să se conecteze la aceste servere, sunt necesare numai adresele IP specifice zonei geografice.

Consola HMC folosește adresele IPv6 următoare pentru a contacta serviciul și suportul IBM când este configurat pentru folosirea conectivității Internet SSL:

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

Folosirea mai multor servere call-home

Aflați ce trebuie să știți atunci când decideți folosirea mai multor servere call-home.

Pentru a evita existența unui punct singular de defectare, configurați consola HMC pentru a folosi mai multe servere call-home. Primul server call-home disponibil încearcă să trateze fiecare eveniment de service. Dacă eșuează conexiunea sau transmisia cu acest server call-home, cererea de service este reîncercată folosind alte servere call-home disponibile, până când încercarea are succes sau au fost încercate toate serverele.

Consola HMC conectată, care a fost identificată de analiza problemelor ca fiind consola de analiză primară pentru un sistem gestionat dat, va raporta problema. Această consolă primară va replica totodată raportul problemei la orice consolă HMC secundară. Această consolă HMC secundară trebuie să fie recunoscută în rețea de consola HMC primară. O consolă HMC secundară este recunoscută de o consolă HMC primară ca un server call-home adițional, atunci când:

- Consola HMC primară este configurată să folosească serverele call-home "descoperite", iar serverul call-home este fie pe aceeași subrețea cu consola primară, fie gestionează același sistem.
- Serverul call-home a fost adăugat manual la lista de console servere call-home disponibile pentru conectivitatea outbound (spre ieșire).

Pregătirea pentru configurarea consolei HMC

Aflați setările de configurare necesare înainte de a începe pașii de configurare.

Pentru a configura consola HMC, trebuie să înțelegeți conceptele înrudite, să luați decizii și să pregătiți informații.

Aflați informațiile de care aveți nevoie pentru a conecta consola HMC la următoarele:

- Procesoarele de service din sistemul gestionat
- Partițiile logice de pe acele sisteme gestionate
- Stații de lucru la distanță
- IBM Service, pentru a implementa funcții "call-home"

Pentru a vă pregăti pentru configurarea HMC, finalizați pașii următori:

1. Obțineți și instalați cel mai recent nivel al versiunii de cod HMC pe care doriți să o instalați.
2. Determinați locul fizic al consolei HMC în relație cu serverele pe care le va gestiona. În cazul în care consola HMC este la mai mult de 8 metri de sistemul gestionat, trebuie să furnizați acces prin browser web la consola HMC din locul sistemul gestionat, astfel încât personalul de service să poată accesa consola HMC.
3. Identificați serverele pe care le va gestiona consola HMC.
4. Determinați dacă veți folosiți o rețea privată sau deschisă pentru a gestiona serverele. Dacă decideți să folosiți o rețea privată, folosiți DHCP, dacă nu folosiți o configurație CSM. CSM nu oferă suport pentru IPv6. Pentru a accesa CSM, trebuie să aveți două rețele. Pentru informații suplimentare despre CSM, consultați documentația furnizată cu caracteristica respectivă. Pentru informații suplimentare despre rețele private și deschise, consultați [“Selectarea unei rețele private sau deschise”](#) la pagina 61.
5. Dacă veți utiliza o rețea deschisă pentru gestionarea unui FSP, trebuie să setați adresa pentru FSP manual prin intermediul meniurilor ASMI (Advanced System Management Interface). Este recomandată o rețea privată, nerutabilă.
6. Dacă aveți două console HMC, desemnați una consolă HMC primară și cealaltă consolă HMC secundară. Consola HMC primară trebuie să fie mai aproape fizic de mașină și trebuie să fie consola HMC care este configurată ca și server call home.
7. Determinați setările de rețea de care veți avea nevoie pentru a conecta consola HMC la stații de lucru la distanță, partiții logice și dispozitive de rețea.
8. Definiți cum va face consola HMC “call home”. Opțiunile de call home includ: peste o conexiune doar de ieșire SSL, peste un modem sau peste o conexiune VPN.
9. Determinați utilizatorii consolei HMC pe care îi veți crea și parolele lor, precum și ce roluri vor primi. Trebuie să asigurați utilizatorilor **hscroot** și **hscpe** o parolă.
10. Documentați următoarele informații de contact ale companiei care vor fi necesare la configurarea call home:
 - Nume companie
 - Contact administrator
 - Adresă de e-mail
 - Numere de telefon
 - Numere de fax
 - Adresa străzii locației fizice a consolei HMC
11. Dacă intenționați să folosiți e-mailul pentru a notifica operatorii sau administratorii de sistem când sunt informații trimise la IBM Service prin call-home, identificați serverul SMTP (Simple Mail Transfer Protocol) și adresele de e-mail pe care le folosiți.
12. Trebuie să definiți următoarele parole:
 - Parola de acces care va fi folosită pentru autentificarea consolei HMC la FSP.
 - Parola de interfață ASMI care va fi folosită de utilizatorul **admin**.
 - Parola de interfață ASMI care va fi folosită de utilizatorul **general**.

Creați parolele când vă conectați de la consola HMC la un nou server pentru prima dată. Dacă HMC este o consolă HMC redundantă sau secundară, obțineți parola de utilizator HMC și pregătiți-vă să o introduceți când vă veți conecta pentru prima dată la FSP-ul serverului gestionat.

Când ați terminat acești pași de pregătire, finalizați [“Foaia de lucru pentru configurarea dinaintea instalării HMC”](#) la pagina 46.

Foia de lucru pentru configurarea dinaintea instalării HMC

Folosiți această foaie de lucru pentru a obține informațiile de instalare de care aveți nevoie, pregătite în vederea instalării.

Politica de parolă îmbunătățită pentru HMC

Trebuie să utilizați o parolă nouă când utilizați prima dată sisteme produse recent cu HMC versiunea 9.940.0 sau ulterioară și după o resetare a sistemului la valorile din fabrică. Această modificare a politicii ajută la schimbarea parolei pentru consola HMC, astfel încât consola să nu rămână cu o parolă cunoscută de toată lumea.

Cu HMC Versiunea 9.940.0 și versiunile ulterioare, parola `hscroot` este expirată și trebuie să fie schimbată ca să puteți accesa funcțiile consolei HMC. Pentru informații suplimentare despre schimbarea parolei, vedeți https://www.ibm.com/support/knowledgecenter/POWER9/p9eh6/p9eh6_useridsandpassword.htm. Însă, dacă modernizați de la un nivel anterior de HMC sau instalare operațională, nu trebuie să schimbați parola.

Setările rețelei

Interfață LAN: Alegeți adaptoarele disponibile (cum ar fi `eth0`, `eth1`) care vor fi folosite de către această consolă HMC pentru conectarea la sisteme gestionate, partiții logice, service și suport și la utilizatorii de la distanță. Pentru informații suplimentare, vedeți “Conexiunile de rețea HMC” la pagina 36. Conectivitatea de la consola HMC poate fi printr-o rețea privată sau deschisă.

Viteză și duplex pentru adaptorul Ethernet

Introduceți viteza dorită și modul duplex pentru adaptorul Ethernet. Opțiunea de detectare automată determină opțiunea optimă în cazul în care nu sunteți sigur ce viteză și mod duplex sunt cele mai bune pentru hardware-ul dumneavoastră. Viteza de mediu (setată implicit la Autodetection) specifică viteza în modul duplex a unui adaptor Ethernet. Selectați Autodetection cu excepția cazului în care aveți o cerință privind specificarea unei viteze fixe. Orice dispozitiv conectat la FSP (switch-uri/HMC), trebuie să fie setat la modul Auto (Speed) / Auto (Duplex), aceasta fiind setarea implicită pentru FSP, care nu poate fi modificată.

Tabela 10. Viteză și duplex pentru adaptorul Ethernet				
Caracteristică	eth0	eth1	eth2	eth3
Selectați viteza și modul duplex				
Viteză mediu (Autodetection, 10/100/1000 Full/ Half Duplex)				

Pentru informații suplimentare despre rețele private și deschise, consultați “Rețele private și deschise în mediul de lucru al consolei HMC” la pagina 38.

Tabela 11. Rețea privată sau deschisă				
Caracteristică	eth0	eth1	eth2	eth3
Specificați rețea Private sau Open pentru fiecare adaptor.				

DHCP (Dynamic Host Configuration Protocol) asigură o metodă automată de configurare a clienților dinamici. Puteți specifica această consolă HMC ca server DHCP. Dacă aceasta este prima sau singura consolă HMC din rețeaua privată, activați consola HMC ca server DHCP. Când activați consola HMC ca server DHCP, sistemele gestionate din rețea vor fi configurate și descoperite automat de HMC.

Pentru adaptoarele Ethernet specificate ca rețele private, completați tabela următoare:

Tabela 12. Server DHCP		
Caracteristici	eth0	eth1
Doriți să specificați această consolă HMC ca server DHCP? (da/nu)		
Dacă da, înregistrați intervalul de adrese IP pe care vreți să-l folosiți.		

Dacă folosiți HCM-ul 7063-CR1, trebuie să conectați portul Ethernet **IPMI** la o rețea pentru a accesa controlerul de gestionare placă de bază (BMC) la HMC. Pentru informații suplimentare, vedeți [“Configurarea conectivității BMC” la pagina 62](#). Completați următoarea tabelă pentru conexiunea dumneavoastră BMC.

Tabela 13. Conexiune BMC	
Caracteristici	IPMI
Doriți să configurați această conexiune prin modul DHCP? (da/nu)	
Dacă nu, listați mai jos adresele statice specificate:	
Adresa IP:	
Masca de subrețea:	
Gateway:	

Pentru adaptoarele specificate ca rețele *deschise*, completați următoarele tabele. Pentru informații suplimentare despre diferitele versiuni Internet Protocol, consultați [“Configurarea tipurilor de rețea consolă HMC” la pagina 56](#).

Utilizarea IPv6

Dacă folosiți IPv6, luați legătura cu administrator rețelei și decideți cum vreți să obțineți adresele IP. Apoi, completați următoarele tabele:

Tabela 14. IPv6 (static)				
Caracteristică	eth0	eth1	eth2	eth3
Folosiți o adresă IP alocată static? Dacă da, înregistrați adresa aici.				

Tabela 15. IPv6 (server DHCP)				
Caracteristică	eth0	eth1	eth2	eth3
Obțineți adresele IP de la un server DHCP? (Da/Nu)				

Tabela 16. IPv6 (ruter IPv6)				
Caracteristică	eth0	eth1	eth2	eth3
Obțineți adresele IP de la un ruter IPv6?				

Pentru informații suplimentare despre setarea adreselor IPv6, vedeți [“Setarea adresei IPv6”](#) la pagina 62. Pentru informații suplimentare despre folosirea exclusivă a adreselor IPv6, vedeți [“Folosirea exclusivă a adreselor IPv6”](#) la pagina 63.

Utilizarea IPv4

Completați tabelele următoare pentru adaptoarele Ethernet specificate ca rețele deschise folosind IPv4.

Tabela 17. IPv4				
Caracteristici	eth0	eth1	eth2	eth3
Doriți să obțineți automat o adresă IP? (da/nu)				
Dacă nu, listați adresa specificată mai jos:				
Adresă interfață TCP/IP:				
Mască rețea interfață TCP/IP:				
Setări firewall:				
Doriți să configurați setările firewall-ului HMC? (da/nu)				
Dacă da, listați aplicațiile și adresele IP care vor fi permise prin firewall:				

Informații TCP/IP

Pentru fiecare nod este necesară o adresă TCP/IP unică, atât pentru Support Element (SE), cât și pentru Hardware Management Console (HMC). Mască de rețea alocată este folosită pentru a genera implicit o adresă unică pentru rețeaua locală privată. Dacă nodurile vor fi conectate într-o rețea mai mare cu o adresă TCP/IP administrată, puteți specifica adresa TCP/IP ce urmează să fie folosită. Cea implicită este generată de sistem.

Setările de firewall

Setările firewall-ului HMC creează o barieră de securitate care permite sau refuză accesul la anumite aplicații de rețea de pe HMC. Puteți specifica aceste setări de control individual pentru fiecare interfață de rețea fizică, ceea ce vă permite să controlați ce aplicații de rețea HMC pot fi accesate în fiecare rețea.

Dacă ați configurat cel puțin un adaptor ca adaptor de rețea deschisă, trebuie să furnizați următoarele informații suplimentare pentru a permite consolei dumneavoastră HMC să acceseze rețeaua locală:

<i>Tabela 18. Adaptor de rețea deschisă</i>	
Informații gazdă locală	
Nume gazdă HMC:	
Nume domeniu:	
Descriere HMC:	
Informații gateway	
Adresă gateway: (nnn.nnn.nnn.nnn)	
Dispozitiv gateway:	
Activare DNS	
Doriți să folosiți DNS? (da/nu)	
Dacă "da", specificați mai jos ordinea de căutare a serverului DNS:	
1.	
2.	
Ordine de căutare sufixe de domeniu:	
1.	
2.	

Informații gazdă locală

Pentru identificarea consolei HMC (Hardware Management Console) în rețea, introduceți numele de gazdă și numele de domeniu pentru HMC. Cu excepția cazului în care folosiți numai nume scurte de gazdă în rețea, introduceți un nume de gazdă complet calificat. Exemplu de nume de domeniu: name.yourcompany.com

Informații gateway

Pentru a defini un gateway implicit, completați adresa TCP/IP care va fi folosită pentru rutarea pachetelor IP. Adresa de gateway informează fiecare calculator sau dispozitiv din rețea unde să trimită date dacă stația țintă nu se află în aceeași subrețea cu sursa.

Activare DNS

DNS-ul este folosit pentru a asigura o convenție de numire standard pentru localizarea calculatoarelor bazate pe IP. Definind server DNS, puteți folosi nume de gazdă pentru a identifica serverele și consolele HMC, în loc să folosiți adrese IP.

Ordine de căutare DNS

Introduceți adresele IP ale serverelor DNS care vor fi căutate pentru maparea numelor de gazdă și a adreselor IP. Această ordine de căutare este disponibilă numai când este activat DNS.

Ordine de căutare sufixe de domeniu

Introduceți sufixele de domeniu pe care le folosiți. Consola HMC folosește sufixe, pe care le anexează numelor necalificate pentru căutărilor DNS. Sufixe sunt căutate în ordinea în care sunt listate. Această ordine de căutare este disponibilă numai când este activat DNS.

Notificare e-mail

Introduceți informațiile de contact prin e-mail dacă doriți să fiți notificat prin e-mail atunci când apar probleme de hardware pe sistemele dumneavoastră.

<i>Tabela 19. Notificare e-mail</i>	
Caracteristici	Câmp de intrare
Adresă e-mail:	

Tabela 19. Notificare e-mail (continuare)	
Caracteristici	Câmp de intrare
Server SMTP:	
Port:	
Erorile pentru care se face notificarea:	
Numai probleme call-home	
Toate problemele	

Server SMTP

Introduceți adresa SMTP (simple mail transfer Protocol) a serverului care trebuie să fie notificat despre un eveniment de sistem. Un exemplu de nume de server SMTP este `relay.us.ibm.com`.

SMTP este protocolul utilizat pentru trimiterea poștei. Când se utilizează SMTP, un client trimite un mesaj și comunică cu serverul SMTP utilizând protocolul SMTP.

Dacă nu cunoașteți adresa serverului SMTP sau nu sunteți sigur, luați legătura cu administratorul rețelei.

Port

Introduceți numărul de port al serverului unde se face notificarea unui eveniment de sistem sau folosiți portul implicit.

Adresele de e-mail pentru notificare

Introduceți adresele de e-mail pentru notificarea la apariția unui eveniment de sistem.

- Selectați **Only call-home problem events** pentru a primi notificarea numai atunci când apar evenimente care creează o funcție call-home.
- Selectați **All problem events** pentru a primi notificarea atunci când apare orice eveniment.

Informații de contact pentru service

Tabela 20. Informații de contact pentru service	
Caracteristici	Câmp de intrare
Nume companie	
Nume administrator	
Adresă de e-mail	
Număr de telefon	
Număr de telefon alternativ	
Număr fax	
Număr de telefon alternativ	
Adresă stradală	
Adresă stradală 2	
Oraș sau localitate	
State	
Cod poștal	
Țară sau regiune	

Tabela 20. Informații de contact pentru service (continuare)

Caracteristici	Câmp de intrare
Loc HMC (dacă este adresa de administrator de mai sus, specificați "la fel"):	
Adresă stradală	
Adresă stradală 2	
Oraș sau localitate	
State	
Cod poștal	
Țară sau regiune	

Autorizare și conectivitate serviciu

Selectați tipul de conexiune pentru contactul cu furnizorul de servicii. Pentru descrierea acestor metode, inclusiv caracteristicile de securitate și cerințele de configurație, vedeți "Alegerea pentru această consolă HMC a serverelor call-home existente pentru conectarea la organizația de service și suport" la pagina 69.

Tabela 21. Autorizare și conectivitate serviciu

Caracteristici	Câmp de intrare
SSL (Secure Sockets Layer) prin Internet	-----
VPN (Virtual Private Network) prin Internet	-----

SSL (Secure Sockets Layer) prin Internet:

Dacă aveți deja o conexiune la Internet de la consola HMC, o puteți folosi pentru apelarea furnizorului de servicii. Folosind legătura existentă la Internet, vă puteți conecta direct la furnizorul de servicii utilizând criptarea SSL (Secure Sockets Layer). Selectați **Use SSL Proxy** dacă doriți să configurați utilizarea SSL criptat printr-o conexiune indirectă utilizând un proxy SSL.

Tabela 22. SSL

Caracteristici	Câmp de intrare
Se folosește proxy SSL? (da/nu)	
Dacă da, listați informațiile mai jos:	
Adresă:	
Port:	
Autentificare cu proxy SSL?	
Dacă da, listați informațiile mai jos:	
Utilizator:	
Parolă:	

Protocol de conexiune internet utilizat

Pentru informații suplimentare despre diferitele versiuni Internet Protocol, consultați [“Configurarea tipurilor de rețea consolă HMC”](#) la pagina 56.

___ IPv4

___ IPv6

___ IPv4 și IPv6

VPN (Virtual Private Network)

Dacă aveți deja o conexiune la Internet de la consola HMC, o puteți folosi pentru apelarea furnizorului de servicii. Folosind legătura existentă la Internet, vă puteți conecta direct la furnizorul de servicii prin rețeaua privată virtuală (VPN).

Notă: Dacă selectați VPN prin Internet, nu veți mai putea selecta alte opțiuni.

Servere Call-home

Determinați ce console HMC doriți să configurați pentru a se conecta la organizația de service și suport ca servere call-home. Pentru mai multe informații despre folosirea mai multor servere call-home, vedeți [“Folosirea mai multor servere call-home”](#) la pagina 44.

___ Acest HMC

___ Alt HMC

Dacă ați bifat **Another HMC**, listați aici celelalte console HMC care au fost configure ca servere call-home:

<i>Tabela 23. Alte console HMC care au fost configure ca servere call-home</i>	
Listă cu numele de gazdă sau adresele IP ale consolelor HMC care au fost configure ca servere call-home	

Alte avantaje ale suportului

My Systems și Premium Search

<i>Tabela 24. My Systems și Premium Search</i>	
Caracteristici	Câmp de intrare
ID-ul dumneavoastră IBM	_____
ID-urile IBM adiționale	_____

Pentru a accesa informații prețioase de suport personalizat, din secțiunile My Systems și Premium Search ale site-ului web Electronic Services, clienții trebuie să își înregistreze ID-ul IBM cu acest sistem. Dacă nu aveți deja un ID IBM, vă puteți înregistra la www.ibm.com/account/profile pentru a obține unul.

Notă: IBM furnizează funcții web personalizate care folosesc informațiile colectate de aplicația IBM Electronic Service Agent. Pentru a utiliza aceste funcții, trebuie întâi să vă înregistrați pe site-ul web IBM Registration la <http://www.ibm.com/account/profile>.

Pentru a autoriza utilizatorii să utilizeze informațiile Electronic Service Agent pentru a personaliza funcțiile Web, introduceți ID-ul dumneavoastră IBM pe care l-ați înregistrat pe site-ul web IBM Registration. Vizitați <http://www.ibm.com/support/electronic> pentru a vedea ce informații valoroase au la dispoziție beneficiarii care înregistrează un ID IBM pentru sistemele lor.

Configurarea consolei HMC

Aflați cum se configurează conexiunile de rețea, securitatea, aplicațiile de serviciu și unele preferințe ale utilizatorului.

În funcție de nivelul de personalizare pe care intenționați să-l aplicați configurației HMC, aveți mai multe opțiuni pentru setarea consolei HMC pentru a vă satisface necesitățile. vrăjitorul Guided Setup este o unealtă pentru HMC proiectată pentru a simplifica setarea consolei HMC. Puteți alege o cale rapidă, prin intermediul vrăjitorului, pentru a crea repede mediul HMC recomandat sau puteți alege să explorați setările disponibile prin care vă ghidează vrăjitorul. Puteți de asemenea realiza pașii de configurare fără ajutorul vrăjitorului, prin [Configurarea consolei HMC folosind meniurile HMC](#).

Înainte de a porni, adunați informația de configurare necesară de care aveți nevoie pentru a finaliza pașii cu succes. Vedeți [“Pregătirea pentru configurarea consolei HMC”](#) la [pagina 44](#) pentru lista cu informațiile necesare. Când ați terminat pregătirea, asigurați-vă că finalizați [“Foaia de lucru pentru configurarea dinaintea instalării HMC”](#) la [pagina 46](#) și apoi reveniți la această secțiune.

Configurarea HMC utilizând calea rapidă prin vrăjitorul Guided Setup

În majoritatea cazurilor, consola HMC poate fi setată să opereze efectiv folosind multe dintre setările implicite. Folosiți lista de verificare pentru calea rapidă ca să pregătiți consola HMC pentru service. După ce finalizați acești pași, consola HMC va fi configurată ca server DHCP (Dynamic Host Configuration Protocol) într-o rețea privată (conectată direct).

Configurarea HMC folosind meniurile

Această secțiune furnizează o listă completă cu toate taskurile de configurare HMC, care vă îndrumă prin procesul de configurare a HMC. Alegeți această opțiune, dacă preferați să nu folosiți vrăjitorul Guided Setup.

Pentru ca setările de configurare să devină efective, trebuie să reporniți consola HMC, așa că este bine să tipăriți această listă de verificare și să o păstrați lângă dumneavoastră când configurați HMC.

Aceste informații conțin referiri la taskuri care nu sunt incluse în acest document. Puteți accesa Informații IBM Power Systems Hardware pe consola HMC sau pe Internet. Pe HMC, IBM Knowledge Center poate fi accesat în colțul din dreapta-sus al barei de taskuri. Pe web, IBM Knowledge Center poate fi accesat la <https://www.ibm.com/support/knowledgecenter>.

Aceste informații conțin referiri la taskuri care nu sunt incluse în acest PDF. Pentru alte materiale de suport, vedeți secțiunea **Additional Resources** din pagina HMC Welcome.

Cerințele preliminare

Înainte să începeți configurarea consolei HMC folosind meniurile consolei HMC, asigurați-vă că finalizați activitate de pregătire de configurare descrisă în [“Pregătirea pentru configurarea consolei HMC”](#) la [pagina 44](#).

Tabela 25. Taskurile manuale de configurare a consolei HMC și unde puteți găsi informații înrudite	
Task	Unde puteți găsi informații înrudite
1. Porniți consola HMC.	“Pornirea consolei HMC” la pagina 54
2. Setati data și ora.	
3. Modificați parolele predefinite.	
4. Creați utilizatori suplimentari și reveniți la această listă de verificare când ați finalizat acest pas.	
5. Configurați conexiunile de rețea.	“Configurarea tipurilor de rețea consolă HMC” la pagina 56

Tabela 25. Taskurile manuale de configurare a consolei HMC și unde puteți găsi informații înrudite (continuare)

Task	Unde puteți găsi informații înrudite
6. Pentru consola HMC modelul 7063-CR1, trebuie să configurați adresa IP a BMC (Baseboard Management Controller).	“Configurarea conectivității BMC” la pagina 62
7. Dacă folosiți o rețea deschisă și o adresă IP fixă, setați informațiile de identificare.	
8. Dacă folosiți o rețea deschisă și o adresă IP fixă, configurați o intrare de rutare ca gateway implicit.	“Configurarea unei intrări de rutare ca gateway implicit” la pagina 64
9. Dacă folosiți o rețea deschisă și o adresă IP fixă, configurați serviciile de nume de domenii.	“Configurarea serviciilor de nume de domeniu” la pagina 65
10. Dacă folosiți o adresă IP fixă și DNS este activat, configurați sufixele de domeniu.	“Configurarea sufixelor de domeniu” la pagina 65
11. Configurați serverul pentru conectarea la organizația IBM de service și suport și reveniți la această listă de verificare după ce ați finalizat acest pas.	“Configurarea consolei locale pentru a raporta erorile la organizația de service și suport” la pagina 67
12. Configurați Events Manager pentru Call Home.	“Configurarea Events Manager for Call Home” la pagina 71
13. Conectați sistemul gestionat la o sursă de alimentare.	
14. Setati parole pentru sistemul gestionat și fiecare din parolele ASMI (general și admin)	“Setarea parolelor pentru sistemul gestionat” la pagina 72
15. Accesați interfața ASMI pentru a seta data și ora pe sistemul gestionat.	
16. Porniți sistemul gestionat și reveniți la această listă de verificare când ați terminat acest pas.	
17. Asigurați-vă că aveți o partiție logică pe sistemul gestionat.	
18. Opțional: adăugați alt sistem gestionat și reveniți la această listă de verificare când ați finalizat acest pas.	
19. Opțional: Dacă instalați un server nou cu HMC, configurați partițiile logice și instalați sistemul de operare.	
20. Dacă nu instalați un server nou acum, realizați taskuri opționale post-configurare pentru a personaliza suplimentar configurația.	“Pașii post-configurare” la pagina 73

Pornirea consolei HMC

Vă puteți loga în consola HMC și alege ce limbă vreți să fie afișată în interfață. Folosiți ID-ul de utilizator implicit hscroot și parola abc123 pentru a vă loga prima dată la HMC.

Despre acest task

Pentru a porni HMC, aplicați procedura următoare:

Procedură

1. Porniți consola HMC apăsând butonul de pornire.
2. Dacă limba dumneavoastră preferată este engleza, continuați cu pasul 4.
Dacă preferați altă limbă decât engleza, tastați numărul **2** când sunteți promptat să modificați locale-ul.
- Notă:** Acest prompt intră în 30 de secunde dacă nu acționați.
3. Selectați locale-ul dorit pentru afișare din lista din fereastra **Selecție locale** și faceți clic pe **OK**.
Locale-ul identifică limba pe care o folosește interfața HMC.
4. Faceți clic pe **Log on and launch the Hardware Management Console web application**.
5. Logați-vă în HMC cu următoarele valori de ID și parolă de utilizator implicite:

ID: hscroot

Parolă: abc123

HMC Enhanced

Afișează mai noua interfață GUI îmbunătățită, cu caracteristici PowerV îmbunătățite.

HMC Classic

Afișează interfața GUI standard, fără caracteristicile PowerVM îmbunătățite.

Notă: Atunci când HMC funcționează ca server DHCP, HMC folosește parola implicită la conectarea la procesorul service pentru prima oară.

6. Apăsați Enter.

Schimbarea datei și orei

Ceasul alimentat de la baterie ține evidența datei și orei pentru consola (HMC). Atunci când înlocuiți bateria sau vă mutați fizic sistemul în alt fus orar, este necesară resetarea datei și a orei consolei. Vedeți cum puteți să modificați data și ora pentru HMC

Despre acest task

Dacă modificați data, ora și fusul orar, modificarea nu afectează sistemele și partițiile logice pe care le gestionează HMC.

Pentru a modifica data și ora pentru HMC, finalizați următorii pași:

Procedură

1. Asigurați-vă că sunteți membru al unuia dintre următoarele roluri:
 - Super administrator
 - Reprezentant de service
 - Operator
 - Vizualizator
2. În zona de navigare, faceți clic pe pictograma **HMC Management**  și apoi selectați **Console Settings**.
3. În zona de conținut, selectați **Change Date and Time**.
4. Dacă selectați **UTC** în câmpul **Clock**, setarea timpului se va ajusta automat pentru ora de vară, în fusul orar pe care îl selectați. Introduceți data, ora și fusul orar și faceți clic pe **OK**.

Rezultate

Configurarea tipurilor de rețea consolă HMC

Configurați consola HMC astfel încât să poată să comunice cu sistemul gestionat, partițiile logice, utilizatori la distanță și service și suport.

Configurarea setărilor consolei HMC pentru a folosi o rețea deschisă pentru conectare la sistemul gestionat
Configurați consola HMC astfel încât să se poată conecta și să poată gestiona un sistem gestionat folosind o rețea deschisă.

Înainte de a începe

Pentru a configura consola HMC astfel încât să se poată conecta și să poată gestiona un sistem gestionat folosind o rețea deschisă, faceți următoarele:

Tabela 26. Configurarea setărilor consolei HMC pentru a folosi o rețea deschisă pentru conectare la sistemul gestionat	
Task	Unde puteți găsi informații înrudite
1. Decideți ce interfață vreți să folosiți pentru sistemul gestionat. eth0 este preferată.	“Foaia de lucru pentru configurarea dinaintea instalării HMC” la pagina 46
2. Identificați porturile Ethernet pentru consola HMC.	“Identificarea portului Ethernet definit ca eth0” la pagina 59
3. Configurați adaptorul Ethernet realizând următoarele taskuri:	
a. Setăți viteza mediului.	“Setarea vitezei de mediu” la pagina 60
b. Selectați tipul de rețea deschisă.	“Selectarea unei rețele private sau deschise” la pagina 61
c. Setăți adresele statice.	“Setarea adresei IPv6” la pagina 62
d. Setăți firewall-ul.	“Modificarea setărilor de firewall pentru HMC” la pagina 63
e. Configurați gateway-ul implicit.	“Configurarea unei intrări de rutare ca gateway implicit” la pagina 64
f. Configurați DNS.	“Configurarea serviciilor de nume de domeniu” la pagina 65
4. Configurați adaptoarele suplimentare, dacă aveți.	
5. Testați conexiunea între serverul gestionat și consola HMC.	“Testarea conexiunii între consola HMC și sistemul gestionat” la pagina 73

Configurați setările consolei HMC pentru a folosi o rețea privată pentru conectarea la sistemul gestionat
Configurați consola HMC astfel încât să se poată conecta și gestiona un sistem gestionat folosind o rețea privată.

Înainte de a începe

Pentru a configura setările de rețea ale consolei HMC astfel încât să se poată conecta la sistemul gestionat folosind o rețea privată, faceți următoarele:

Tabela 27. Configurați setările consolei HMC pentru a folosi o rețea privată pentru conectarea la sistemul gestionat

Task	Unde puteți găsi informații înrudite
1. Decideți ce interfață vreți să folosiți pentru sistemul gestionat.	“Foaia de lucru pentru configurarea dinaintea instalării HMC” la pagina 46
2. Identificați porturile Ethernet pentru consola HMC.	“Identificarea portului Ethernet definit ca eth0” la pagina 59
3. Configurați consola HMC ca un server DHCP.	“Configurarea consolei HMC ca server DHCP” la pagina 61
4. Testați conexiunea între serverul gestionat și consola HMC.	“Testarea conexiunii între consola HMC și sistemul gestionat” la pagina 73

Configurarea setărilor consolei HMC pentru a folosi o rețea deschisă pentru conectarea la partiții logice

Înainte de a începe

Pentru a configura setările de rețea ale consolei HMC astfel încât să se poată conecta la partiții logice folosind o rețea deschisă, faceți următoarele:

Tabela 28. Configurarea setărilor consolei HMC pentru a folosi o rețea deschisă pentru conectarea la partiții logice

Task	Unde puteți găsi informații înrudite
1. Decideți ce interfață vreți să folosiți pentru sistemul gestionat.	“Foaia de lucru pentru configurarea dinaintea instalării HMC” la pagina 46
2. Identificați porturile Ethernet pentru consola HMC.	“Identificarea portului Ethernet definit ca eth0” la pagina 59
3. Configurați adaptorul Ethernet realizând următoarele taskuri:	
a. Setări viteza mediului.	“Setarea vitezei de mediu” la pagina 60
b. Selectați tipul de rețea deschisă.	“Selectarea unei rețele private sau deschise” la pagina 61
c. Setări adresele statice.	“Setarea adresei IPv6” la pagina 62
d. Setări firewall-ul.	“Modificarea setărilor de firewall pentru HMC” la pagina 63
e. Configurați gateway-ul implicit.	“Configurarea unei intrări de rutare ca gateway implicit” la pagina 64
f. Configurați DNS.	“Configurarea serviciilor de nume de domeniu” la pagina 65
4. Configurați adaptoarele suplimentare, dacă aveți.	
5. Testați conexiunea între serverul gestionat și consola HMC.	“Testarea conexiunii între consola HMC și sistemul gestionat” la pagina 73

Configurarea setărilor consolei HMC pentru a folosi o rețea deschisă pentru conectarea la utilizatori la distanță

Înainte de a începe

Pentru a configura setările de rețea ale consolei HMC astfel încât să se poată conecta la utilizatori la distanță folosind o rețea deschisă, faceți următoarele:

Tabela 29. Configurarea setărilor consolei HMC pentru a folosi o rețea deschisă pentru conectarea la utilizatori la distanță	
Task	Unde puteți găsi informații înrudite
1. Decideți ce interfață vreți să folosiți pentru sistemul gestionat.	“Foaia de lucru pentru configurarea dinaintea instalării HMC” la pagina 46
2. Identificați porturile Ethernet pentru consola HMC.	“Identificarea portului Ethernet definit ca eth0” la pagina 59
3. Configurați adaptorul Ethernet realizând următoarele taskuri:	
a. Setati viteza mediului.	“Setarea vitezei de mediu” la pagina 60
b. Selectați tipul de rețea deschisă.	“Selectarea unei rețele private sau deschise” la pagina 61
c. Setati adresele statice.	“Setarea adresei IPv6” la pagina 62
d. Setati firewall-ul.	“Modificarea setărilor de firewall pentru HMC” la pagina 63
e. Configurați gateway-ul implicit.	“Configurarea unei intrări de rutare ca gateway implicit” la pagina 64
f. Configurați DNS.	“Configurarea serviciilor de nume de domeniu” la pagina 65
g. Configurați sufixele.	“Configurarea sufixelor de domeniu” la pagina 65
4. Configurați adaptoarele suplimentare, dacă aveți.	

Configurarea setărilor serverului call-home HMC

Înainte de a începe

Pentru a configura setările serverului call-home HMC pentru a putea fi raportate problemele, faceți următoarele:

Tabela 30. Configurarea setărilor serverului call-home HMC	
Task	Unde puteți găsi informații înrudite
1. Asigurați-vă că aveți toate informațiile cerute pentru beneficiar	“Foaia de lucru pentru configurarea dinaintea instalării HMC” la pagina 46
2. Configurați această consolă HMC pentru a raporta erorile sau alegeți un server call-home existent pentru a raporta erorile	“Configurarea consolei locale pentru a raporta erorile la organizația de service și suport” la pagina 67 “Alegerea pentru această consolă HMC a serverelor call-home existente pentru conectarea la organizația de service și suport” la pagina 69

Tabela 30. Configurarea setărilor serverului call-home HMC (continuare)

Task	Unde puteți găsi informații înrudite
3. Verificați că funcționează configurația pentru call-home	“Verificarea funcționării conexiunii la organizația de service și suport” la pagina 70
4. Autorizați utilizatorii să vizualizeze datele de sistem colectate	“Autorizarea utilizatorilor pentru a vizualiza datele de sistem colectate” la pagina 70
5. Planificați transmiterea datelor de sistem	“Transmiterea informațiilor de service” la pagina 70

Identificarea portului Ethernet definit ca eth0

Conexiunea Ethernet la serverul gestionat trebuie făcută folosind portul Ethernet care este definit ca eth0 pe consola HMC.

Dacă nu ați instalat adaptoare Ethernet adiționale în sloturile PCI de pe consola HMC, portul Ethernet integrat primar este întotdeauna definit ca eth0 sau eth1 pe HMC, pentru eventualitatea în care doriți să folosiți HMC ca server DHCP pentru sistemele dumneavoastră gestionate.

Dacă ați instalat adaptoare Ethernet adiționale în sloturile PCI, portul definit ca eth0 depinde de locul și tipul adaptoarelor Ethernet pe care le-ați instalat.

Notă: Este posibil ca următoarele reguli generale să nu fie valabile pentru toate configurațiile.

Următoarea tabelă prezintă regulile pentru amplasarea adaptoarelor Ethernet după tipul de consolă HMC.

Tabela 31. Tipurile de consolă HMC și regulile pentru amplasarea adaptoarelor Ethernet

Tip HMC	Reguli pentru amplasarea adaptoarelor Ethernet
Console HMC montate în dulap cu două porturi Ethernet integrate	Consola HMC suportă doar un adaptor Ethernet suplimentar. • Dacă este instalat un adaptor Ethernet adițional, acest port este definit ca eth0. În acest caz, portul Ethernet integrat primar este definit ca eth1, iar portul Ethernet integrat secundar ca eth2.eth2. • Dacă adaptorul Ethernet este un adaptor Ethernet cu port dual, în mod normal portul etichetat Act/Link A va fi eth0. Portul etichetat Act/link B va fi eth1. În acest caz, portul Ethernet integrat primar este definit ca eth2, iar portul Ethernet integrat secundar ca eth3. • Dacă nu sunt instalate adaptoare, portul Ethernet integrat primar este definit ca eth0.

Tabela 31. Tipurile de consolă HMC și regulile pentru amplasarea adaptoarelor Ethernet (continuare)

Tip HMC	Reguli pentru amplasarea adaptoarelor Ethernet
Modele independente cu un singur port Ethernet integrat	Definițiile depind de tipul de adaptor Ethernet pe care l-ați instalat: • Dacă este instalat un singur adaptor Ethernet, acest adaptor este definit ca eth0. • Dacă adaptorul Ethernet este un adaptor Ethernet cu port dual, portul etichetat Act/link A va fi eth0. Portul etichetat Act/link B va fi eth1. n acest caz, portul Ethernet integrat primar este definit ca eth2. • Dacă nu sunt instalate adaptoare, portul Ethernet integrat este definit ca eth0. • Dacă au fost instalate mai multe adaptoare Ethernet, vedeți “Determinarea numelui interfeței pentru un adaptor Ethernet” la pagina 60.

Determinarea numelui interfeței pentru un adaptor Ethernet

În cazul în care configurați consola HMC ca server DHCP, acel server poate opera numai pe conectorii NIC (network interface card) pe care HMC îi identifică drept eth0 și eth1. De asemenea, poate fi necesar să stabiliți în ce conector NIC trebuie să introduceți cablul Ethernet. Vedeți cum se determină conectorii NIC pe care consola HMC îi identifică drept eth0 și eth1.

Despre acest task

Pentru a determina numele alocat de HMC unui adaptor Ethernet, procedați în felul următor:

Procedură

1. În zona de navigare, faceți clic pe pictograma **HMC Management**  și apoi selectați **Console Settings**.
2. În panoul de conținut, faceți clic pe **Change Network Settings**.
3. Din fereastra **Change Network Settings** faceți clic pe fila **LAN adapters**. În următorul exemplu de intrare, acest port Ethernet este identificat ca eth0: Ethernet eth0 52:54:00:fa:b6:8e (<IP address of HMC>).
4. Notați rezultatele. Dacă este nevoie să vizualizați sau să schimbați setările adaptorului LAN, faceți clic pe **Details**.
5. Faceți clic pe **OK**.

Setarea vitezei de mediu

Aflați cum să specificați viteza mediului care include viteza și modul duplex ale adaptorului Ethernet.

Înainte de a începe

Implicit pentru setările de adaptor HMC este **Autodetection**. Dacă acest adaptor este conectat la un switch de rețea locală, trebuie să potriviți setările pentru portul switch-ului. Pentru a seta viteza și duplexul, finalizați următorii pași:

Procedură

1. În zona de navigare, faceți clic pe pictograma **HMC Management**  și apoi selectați **Console Settings**.
2. În zona de conținut, selectați **Change network settings**.
3. Faceți clic pe fișa **LAN Adapters**.
4. Selectați adaptorul de LAN cu care doriți să lucrați și faceți clic pe **Details**.
5. În secțiunea de informații pentru rețeaua locală, selectați **Autodetection** sau combinația corespunzătoare pentru viteza mediului și duplex.
6. Faceți clic pe **OK**.

Selectarea unei rețele private sau deschise

O *rețea de service privată* este alcătuită din consola HMC și sistemele gestionate. O rețea de service privată este restricționată la consolele și sistemele pe care le gestionează, fiind separată de rețeaua companiei. O *rețea deschisă* este alcătuită din rețeaua de service privată plus rețeaua companiei. Pe lângă console și sisteme gestionate, o rețea deschisă ar trebui să conțină puncte finale din rețea și ar trebui să se întindă peste mai multe subrețele și dispozitive de rețea.

Despre acest task

Pentru a selecta o rețea privată sau publică, procedați în felul următor:

Procedură

1. În zona de navigare, faceți clic pe pictograma **HMC Management**  și apoi selectați **Console Settings**.
2. În zona de conținut, selectați **Change network settings**.
3. Faceți clic pe fișa **LAN Adapters**.
4. Selectați adaptorul de LAN cu care doriți să lucrați și faceți clic pe **Details**.
5. Faceți clic pe fila **LAN Adapter**.
6. În pagina Local area network information, selectați **Private** sau **Open**.
7. Faceți clic pe **OK**.

Configurarea consolei HMC ca server DHCP

DHCP (Dynamic Host Configuration Protocol) asigură o metodă automată de configurare a clienților dinamici.

Pentru a configura consola HMC ca server DHCP, urmați pașii:

1. În zona de navigare, faceți clic pe pictograma **HMC Management**  și apoi selectați **Console Settings**.
2. În zona de conținut, selectați **Change network settings**. Se deschide fereastra Customize Network Settings.
3. Selectați adaptorul de LAN cu care doriți să lucrați și faceți clic pe **Details**.
4. Selectați **Private** și apoi selectați tipul rețelei.
5. În secțiunea DHCP Server, selectați **Enable DHCP Server** pentru a activa HMC ca server DHCP.

Notă: Puteți configura consola HMC să fie un server DHCP doar într-o rețea privată. Dacă utilizați o rețea deschisă, opțiunea pentru selectare **Enable DHCP** nu este disponibilă.

6. Introduceți intervalul de adrese pentru serverul DHCP.

7. Faceți clic pe **OK**.

Dacă ați configurat consola HMC să fie un server DHCP într-o rețea privată, trebuie să verificați că rețeaua privată este configurată corect. Pentru informații despre cum să conectați consola HMC la o rețea privată, vedeți [“Selectarea unei rețele private sau deschise”](#) la pagina 61.

Pentru informații suplimentare, vedeți [“HMC ca un server DHCP”](#) la pagina 39.

Configurarea conectivității BMC

Puteți configura sau vizualiza setările de rețea de pe BMC pentru consola de gestionare.

Notă: Acest task este aplicabil numai pentru 7063-CR1. Această conexiune este necesară pentru a accesa controlerul de gestionare a plăcii de bază (baseboard management controller - BMC), pe HMC.

Pentru a configura conexiunea BMC, parcurgeți următorii pași:

1. În zona de navigare, faceți clic pe pictograma **HMC Management**  și apoi selectați **Console Settings**.
2. În panoul de conținut, faceți clic pe **Change BMC/IPMI network settings**.
3. Selectați modul de conectare (**DHCP** sau **Static**).

Dacă selectați **Static**, completați următoarele adrese:

- **IP address**
- **Subnet mask**
- **Gateway**

4. Faceți clic pe **OK**.

De asemenea, puteți configura conexiunea BMC la rețea folosind interfața bootloader Petitboot. Pentru informații suplimentare, vedeți [Configurarea adresei IP de firmware](#).

Setarea adresei IPv4

Vedeți cum vă setați adresa IPv4 pe consola HMC.

Procedură

1. În zona de navigare, faceți clic pe pictograma **HMC Management**  și apoi selectați **Console Settings**.
2. În zona de conținut, selectați **Change network settings**.
3. Faceți clic pe fișa **LAN Adapters**.
4. Selectați adaptorul de LAN cu care doriți să lucrați și faceți clic pe **Details**.
5. Faceți clic pe fișa **Basic Settings**.
6. Selectați o adresă IPv4.
7. Dacă ați selectat să specificați o adresă IP, introduceți adresa pentru interfața TCP/IP și masca de rețea pentru interfața TCP/IP.
8. Faceți clic pe **OK**.

Setarea adresei IPv6

Vedeți cum vă setați adresa IPv6 pe consola HMC.

Procedură

1. În zona de navigare, faceți clic pe pictograma **HMC Management**  și apoi selectați **Console Settings**.
2. În zona de conținut, selectați **Change network settings**.
3. Faceți clic pe fișa **LAN Adapters**.
4. Selectați adaptorul de LAN cu care doriți să lucrați și faceți clic pe **Details**.
5. Faceți clic pe fișa **IPv6 Settings**.
6. Selectați opțiunea **Autoconfig** sau adăugați o adresă IP statică.
7. Dacă ați adăugat o adresă IP, introduceți adresa IPv6 și lungimea prefixului și faceți clic pe **OK**.
8. Faceți clic pe **OK**.

Folosirea exclusivă a adreselor IPv6

Vedeți cum puteți să configurați consola HMC astfel încât să folosească numai adrese IPv6.

Procedură

1. În zona de navigare, faceți clic pe pictograma **HMC Management**  și apoi selectați **Console Settings**.
2. În zona de conținut, selectați **Change network settings**.
3. Faceți clic pe fișa **LAN Adapters**.
4. Selectați adaptorul de LAN cu care doriți să lucrați și faceți clic pe **Details**.
5. Selectați **No IPv4 address**.
6. Faceți clic pe fișa **IPv6 Settings**.
7. Selectați **Use DHCPv6 to configure IP settings** sau adăugați adrese IP statice, apoi faceți clic pe **OK**.

Ce se face în continuare

După ce faceți clic pe **OK**, trebuie să restartați consola HMC pentru ca modificările să devină efective.

Modificarea setărilor de firewall pentru HMC

Într-o rețea deschisă, un firewall este folosit pentru a controla accesul din exterior la rețeaua companiei. De asemenea, consola HMC are un firewall pe fiecare dintre adaptoarele Ethernet. Pentru a controla HMC de la distanță sau pentru a acorda acces la distanță altora, modificați setările firewall ale adaptorului Ethernet de pe consola HMC care este conectată la rețeaua deschisă.

Despre acest task

Pentru a configura un firewall, folosiți pașii următori:

Procedură

1. În zona de navigare, faceți clic pe pictograma **HMC Management**  și apoi selectați **Console Settings**.
2. În zona de conținut, selectați **Change network settings**.
3. Faceți clic pe fișa **LAN Adapters**.
4. Selectați adaptorul de LAN cu care doriți să lucrați și faceți clic pe **Details**.
5. Faceți clic pe fișa **Firewall**.

6. Folosind una dintre metodele următoare, puteți permite ca prin firewall să treacă orice adresă IP care folosește o anumită aplicație sau puteți specifica una sau mai multe adrese IP:
 - Permitearea trecerii prin firewall a oricărei adrese IP care folosește o anumită aplicație:
 - a. În caseta de sus, evidențiați aplicația.
 - b. Faceți clic pe **Allow Incoming**. Aplicația este afișată în caseta de jos, indicându-se că a fost selectată.
 - Specificarea adreselor IP care pot trece prin firewall:
 - a. În caseta de sus, evidențiați o aplicație.
 - b. Faceți clic pe **Allow Incoming by IP Address**.
 - c. În fereastra Hosts Allowed, introduceți adresa IP și masca de rețea.
 - d. Faceți clic pe **Add** și apoi pe **OK**.
7. Faceți clic pe **OK**.

Activarea accesului shell restricționat de la distanță

Puteți să activați accesul shell restricționat de la distanță atunci când configurați un firewall.

Despre acest task

Pentru a activa accesul shell restricționat de la distanță, procedați în felul următor:

Procedură

1. În zona de navigare, faceți clic pe **HMC Management**.
2. Faceți clic pe **Remote Command Execution**.
3. Selectați **Enable remote command execution using the ssh facility** și apoi faceți clic pe **OK**.

Ce se face în continuare

Acum accesul shell restricționat de la distanță este activat.

Activarea accesului web de la distanță

Puteți să activați accesul web de la distanță pe consola dumneavoastră HMC.

Despre acest task

Pentru a activa accesul web de la distanță, procedați în felul următor:

Procedură

1. În zona de navigare, faceți clic pe **HMC Management**.
2. Faceți clic pe **Remote Operation**.
3. Selectați **Enable** și apoi faceți clic pe **OK**.

Ce se face în continuare

Acum accesul web de la distanță este activat.

Configurarea unei intrări de rutare ca gateway implicit

Vedeți cum se configurează o intrare de rutare ca gateway implicit. Acest task este disponibil atunci când utilizați o rețea deschisă.

Înainte de a începe

Pentru a configura o intrare de rutare ca gateway implicit, procedați în felul următor:

Procedură

1. În zona de navigare, faceți clic pe pictograma **HMC Management**  și apoi selectați **Console Settings**.
2. În zona de conținut, selectați **Change network settings**. Se deschide fereastra Customize Network Settings.
3. Faceți clic pe fișa **Routing**.
4. În secțiunea de informații Gateway implicit, introduceți adresa gateway și dispozitivul gateway pentru intrarea de rutare pe care vreți să o setați ca gateway implicit.
5. Faceți clic pe **OK**.

Configurarea serviciilor de nume de domeniu

Dacă intenționați să configurați o rețea deschisă, configurați serviciile de nume de domeniu.

Despre acest task

Dacă intenționați să configurați o rețea deschisă, configurați serviciile de nume de domeniu. Sistemul de nume de domeniu (Domain Name System - DNS) este un sistem de bază de date distribuită, pentru gestionarea numelor de gazdă și a adreselor IP (Internet Protocol) asociate. Configurarea serviciilor de nume de domeniu include activarea DNS-ului și specificarea ordinii de căutare a sufixelor de domeniu.

Procedură

1. În zona de navigare, faceți clic pe pictograma **HMC Management**  și apoi selectați **Console Settings**.
2. În zona de conținut, selectați **Change network settings**. Se deschide fereastra Change Network Settings.
3. Faceți clic pe fișa **Name Services**.
4. Selectați **DNS enabled** pentru a activa DNS.
5. Specificați serverul DNS și ordinea de căutare a sufixului de domenii și apăsați **Adăugare**.
6. Faceți clic pe **OK**.

Configurarea sufixelor de domeniu

Lista sufixelor de domeniu este folosită pentru a rezolva o adresă IP începând cu prima intrare din listă.

Despre acest task

Sufixul de domeniu este un șir adăugat la sfârșitul unui nume de gazdă pentru a ajuta la rezolvarea adresei sale IP. De exemplu, este posibil ca numele de gazdă myname să nu poată fi rezolvat. Însă dacă șirul myloc.mycompany.com este un element din tabelul cu sufixele de domeniu, atunci se va încerca să se rezolve myname.mloc.mycompany.com.

Pentru a configura o intrare de sufix de domeniu, folosiți pașii următori:

Procedură

1. În zona de navigare, faceți clic pe pictograma **HMC Management**  și apoi selectați **Console Settings**.
2. În zona de conținut, selectați **Change network settings**. Se deschide fereastra Customize Network Settings.

3. Faceți clic pe fișa **Name Services**.
4. Introduceți un șir care să fie folosit ca o intrare de sufix de domeniu.
5. Faceți clic pe **Add** pentru a-l adăuga în listă.

Configurarea consolei HMC pentru a folosi autentificarea la distanță LDAP

Puteți configura consola HMC (Hardware Management Console), astfel încât să folosească autentificarea la distanță LDAP (Lightweight Directory Access Protocol).

Înainte de a începe

Când un utilizator se loghează la HMC, prima dată autentificarea se face cu un fișier de parole local. Dacă nu este găsit un fișier de parole local, consola HMC poate contacta pentru autentificare un server LDAP la distanță. Trebuie să configurați consola HMC pentru a folosi autentificarea LDAP la distanță.

Notă: Înainte de a configura consola HMC ca să folosească autentificarea la distanță Kerberos, trebuie să vă asigurați că există o conexiune de rețea funcțională între consola HMC și serverele LDAP. Pentru informații suplimentare despre cum să configurați conexiunile de rețea ale consolei HMC, vedeți [“Configurarea tipurilor de rețea consolă HMC”](#) la pagina 56.

Despre acest task

Pentru a configura consola HMC ca să folosească autentificarea LDAP, finalizați următorii pași:

Procedură

1. În zona de navigare, faceți clic pe pictograma **Users and Security**  și apoi selectați **Systems and Console Security**.
2. În panoul de conținut, selectați **Manage LDAP**. Se deschide fereastra LDAP Server Definition.
3. Selectați **Enable LDAP**.
4. Definiți un server LDAP pe care să-l folosiți pentru autentificare.
5. Definiți atributul LDAP care este folosit pentru a identifica utilizatorul autentificat. Implicit este **uid**, dar puteți folosi propriile atribute.
6. Definiți arborele numelui distinctiv, cunoscut și ca baza de căutare, pentru serverul LDAP.
7. Faceți clic pe **OK**.
8. Dacă un utilizator vrea să folosească autentificarea LDAP, utilizatorul trebuie să configureze profilurile astfel încât să folosească autentificarea la distanță LDAP în loc de autentificarea locală.

Configurarea consolei HMC pentru a folosi serverele KDC (Key Distribution Center) pentru autentificarea la distanță Kerberos

Puteți configura consola HMC să folosească serverele KDC (Key Distribution Center) pentru autentificarea la distanță Kerberos

Înainte de a începe

Când un utilizator se loghează la HMC, prima dată autentificarea se face cu un fișier de parole local. Dacă nu este găsit un fișier de parole local, consola HMC poate contacta pentru autentificare un server Kerberos la distanță. Trebuie să configurați consola HMC pentru a folosi autentificarea Kerberos la distanță.

Notă: Înainte de a configura consola HMC ca să folosească autentificarea la distanță Kerberos, trebuie să vă asigurați că există o conexiune de rețea funcțională între consola HMC și serverele KDC. Pentru informații suplimentare despre cum să configurați conexiunile de rețea ale consolei HMC, vedeți [“Configurarea tipurilor de rețea consolă HMC”](#) la pagina 56.

Despre acest task

Pentru a configura consola HMC pentru a folosi serverele KDC pentru autentificarea Kerberos la distanță, finalizați pașii următori:

Procedură

1. Activați serviciul NTP (Network Time Protocol) pe consola HMC și setați consola HMC și serverele KDC astfel încât să-și sincronizeze ceasurile cu același server NTP. Pentru a activa serviciul NTP pe consola HMC, faceți următoarele:
 - a) În zona de navigare, faceți clic pe pictograma **HMC Management**  și apoi selectați **Console Settings**.
 - b) În panoul de conținut, selectați **Change Date and Time**.
 - c) Selectați fișa **NTP Configuration**.
 - d) Selectați **Enable NTP service on this HMC**.
 - e) Faceți clic pe **OK**.
2. Configurați fiecare profil de utilizator al consolei HMC ca se folosească autentificarea la distanță Kerberos în locul autentificării locale.
3. Opțional, puteți importa un fișier cheie-serviciu în HMC. Fișierul cheie-serviciu conține principalul gazdei de identificare a consolei HMC la serverul KDC. Fișierele cheie-serviciu mai sunt cunoscute și ca *keytabs* (tabele de chei). Pentru a importa un fișier cheie-serviciu pe consola HMC, faceți următoarele:

- a) În zona de navigare, faceți clic pe pictograma **Users and Security**  și apoi selectați **Systems and Console Security**.
 - b) În panoul de conținut, selectați **Manage KDC**.
 - c) Selectați **Actions > Import Service Key**. Se deschide fereastra Import Service Key.
 - d) Introduceți locația fișierului de cheie-serviciu.
 - e) Faceți clic pe **OK**.
4. Adăugați un nou server KDC la această consolă HMC. Pentru a adăuga un nou server KDC la această consolă HMC, urmați pașii:

- a) În zona de navigare, faceți clic pe pictograma **Users and Security**  și apoi selectați **Systems and Console Security**.
- b) În panoul de conținut, selectați **Manage KDC**.
- c) Selectați **Actions > Add KDC Server**. Se deschide fereastra Import Service Key.
- d) Introduceți numele regiunii (realm) și de gazdă sau adresa IP a serverului KDC.
- e) Faceți clic pe **OK**.

Configurarea consolei locale pentru a raporta erorile la organizația de service și suport

Configurați acest HMC astfel încât să poată raporta erori de apelare acasă folosind conectivitatea LAN.

Configurarea consolei HMC pentru a se conecta la organizația de service și suport folosind vrăjitorul de setare call-home

Configurați consola HMC ca să fie un server call-home folosind vrăjitorul call-home.

Înainte de a începe

Această procedură vă arată cum configurați consola HMC ca server call-home folosind conexiuni la Internet directe (bazate pe LAN) și indirecte (SSL).

Înainte de a începe acest task, asigurați-vă că:

- Administratorul de rețea a verificat că este permisă conectivitatea. Pentru informații suplimentare, vedeți [“Pregătirea pentru configurarea consolei HMC”](#) la pagina 44.
- În cazul în care configurați suportul Internet printr-un server proxy, trebuie să aveți următoarele:
 - Adresa IP și portul serverului proxy
 - Informațiile de autentificare proxy
- Adaptorul desemnat ca **eth1** (cel care este desemnat ca rețea deschisă) este folosit. Pentru informații suplimentare, vedeți [“Alegerea setărilor de rețea pe HMC”](#) la pagina 36.
- Un cablu Ethernet care conectează fizic HMC la LAN.

Pentru a configura consola HMC ca să fie un server call-home folosind vrăjitorul call-home, urmați pașii:

Procedură



1. În zona de navigare, faceți clic pe pictograma **Serviceability** și apoi selectați **Service Management**.
2. În panoul de conținut, faceți clic pe **Call-Home Setup Wizard**. Se deschide fereastra Connectivity and Call-Home Servers wizard. Urmăriți instrucțiunile din vrăjitor pentru a configura serverul call-home.

Configurarea consolei locale pentru a raporta erorile la organizația de service și suport

Configurați acest HMC astfel încât să poată raporta erori de apelare acasă folosind conectivitatea LAN.

Configurarea consolei HMC pentru a contacta organizația de service și suport folosind Internet bazat pe LAN și SSL

Vedeți cum puteți să configurați consola HMC ca server call-home folosind conexiuni la Internet directe (bazate pe LAN) și indirecte (SSL).

Înainte de a începe

Înainte de a începe acest task, asigurați-vă că:

- Administratorul de rețea a verificat că este permisă conectivitatea. Pentru informații suplimentare, vedeți [“Pregătirea pentru configurarea consolei HMC”](#) la pagina 44.
- Au fost configurate informațiile de contact ale beneficiarului. Verificați informațiile de contact intrând în interfața HMC și făcând clic pe **Serviceability > Service Management > Manage Customer Information**.
- În cazul în care configurați suportul pentru internet printr-un server proxy, trebuie de asemenea să aveți următoarele informații:
 - Adresa IP și portul serverului proxy
 - Informațiile de autentificare proxy
- Trebuie să aveți cel puțin o interfață de rețea deschisă configurată. Pentru informații suplimentare, vedeți [“Rețele private și deschise în mediul de lucru al consolei HMC”](#) la pagina 38.
- Un cablu Ethernet care conectează fizic HMC la LAN.

Despre acest task

Pentru a configura consola HMC ca un server Call Home utilizând Internet bazat pe LAN și SSL, urmați pașii:

Procedură



1. În zona de navigare, faceți clic pe pictograma **Serviceability** și apoi selectați **Service Management**.
2. În secțiunea Connectivity, faceți clic pe **Manage Outbound Connectivity**. Se deschide fereastra Call-home Server Consoles.
3. Faceți clic pe **Configure**.
4. În fereastra Outbound Connectivity Settings, bifați **Enable local system as call-home server**.
5. Acceptați acordul.
6. În fereastra Outbound Connectivity Settings, selectați pagina **Internet**.
7. Bifați caseta **Allow an existing internet connections for service**.
8. Dacă folosiți un proxy SSL, bifați caseta **Use SSL proxy**.
9. Dacă folosiți un proxy SSL, completați adresa de proxy și portul. Obțineți aceste informații de la administratorul de rețea.
10. Dacă ați bifat **Use SSL proxy** și proxy-ul necesită autentificarea cu ID de utilizator și parolă, bifați caseta **Authenticate with the SSL proxy**. Tastați ID-ul de utilizator și parola. Obțineți ID-ul de utilizator și parola de la administratorul de rețea.
11. Selectați **Protocol to Internet** pe care vreți să-l folosiți.
12. Pe pagina **Internet**, faceți clic pe **Test**.
13. În fereastra Test Internet, faceți clic pe **Start**.
14. Verificați dacă testul este finalizat cu succes.
15. În fereastra Test Internet, faceți clic pe **Cancel**.
16. În fereastra Outbound Connectivity Settings, faceți clic pe **OK**.

Alegerea pentru această consolă HMC a serverelor call-home existente pentru conectarea la organizația de service și suport

Alegeți servere call-home HMC existente, care au fost recunoscute sau descoperite de această consolă HMC pentru a le raporta erorile.

Înainte de a începe

Consolele HMC descoperite sunt acele console HMC care sunt activate ca servere call-home și care fie sunt în aceeași subrețea, fie gestionează același sistem ca această consolă HMC.

Pentru a alege o consolă HMC să fie serverul call-home atunci când această consolă raportează erorile, faceți următoarele:

Procedură



1. În zona de navigare, faceți clic pe pictograma **Serviceability** și apoi selectați **Service Management**.
2. În panoul de conținut, faceți clic pe **Manage Outbound Connectivity**. Se deschide fereastra Call-Home Server Consoles.
3. Faceți clic pe **Use discovered call-home server consoles**. Consola HMC afișează adresele IP sau numele de gazdă pentru consolele HMC configurate pentru call-home.
4. Faceți clic pe **OK**.

Rezultate

Puteți adăuga și manual servere call-home HMC existente care sunt pe alte subrețele. Selectați adresa IP sau numele de gazdă al consolei HMC care este configurată pentru call-home apoi faceți clic pe **Add** și apoi faceți clic pe **OK**.

Verificarea funcționării conexiunii la organizația de service și suport

Se verifică raportarea problemelor, pentru a se stabili dacă funcționează conexiunea la organizația de service și suport.

Despre acest task

Pentru a verifica funcționarea configurației call-home, procedați în felul următor:

Procedură

1. În zona de navigare, faceți clic pe pictograma **Serviceability**  și apoi selectați **Service Management**.
2. În panoul de conținut, faceți clic pe **Create Event**.
3. Selectați **Test Automatic problem Reporting** și introduceți un comentariu.
4. Faceți clic pe **Request Service**. Așteptați câteva minute pentru a fi trimisă cererea.
5. În fereastra Service Management, selectați **Manage Events**.
6. Selectați **All open problems**.
7. Verificați că un eveniment PMH și un număr este alocat numărului de problemă pe care l-ați deschis.
8. Selectați acel eveniment și faceți clic pe **Close**.
9. În fereastra **Close** introduceți-vă numele și un scurt comentariu.

Autorizarea utilizatorilor pentru a vizualiza datele de sistem colectate

Trebuie să autorizați utilizatorii pentru a putea vedea datele despre sisteme.

Înainte de a începe

Înainte de a autoriza utilizatorii pentru a vizualiza datele colectate despre sisteme, trebuie să obțineți un ID IBM. Pentru informații suplimentare despre modul în care puteți să obțineți un ID IBM, vedeți [“Foaia de lucru pentru configurarea dinaintea instalării HMC” la pagina 46](#).

Despre acest task

Pentru a autoriza utilizatorii să vadă datele colectate ale sistemelor, faceți următoarele:

Procedură

1. În zona de navigare, faceți clic pe pictograma **Serviceability**  și apoi selectați **Service Management**.
2. În panoul de conținut, selectați **Authorize User**.
3. Introduceți-vă ID-ul IBM.
4. Faceți clic pe **OK**.

Transmiterea informațiilor de service

Puteți să transmiteți informații la furnizorul de servicii imediat sau puteți să planificați ca informațiile să fie transmise la intervale regulate.

Înainte de a începe

IBM furnizează funcții web personalizate care folosesc informațiile colectate de IBM Electronic Service Agent. Pentru a utiliza aceste funcții, trebuie întâi să vă înregistrați pe site-ul web IBM Registration la <http://www.ibm.com/account/profile>. Pentru a autoriza utilizatorii să folosească informațiile Electronic Service Agent pentru a personaliza funcțiile web, vedeți “Autorizarea utilizatorilor pentru a vizualiza datele de sistem colectate” la pagina 70. Pentru informații suplimentare despre avantajele înregistrării unui ID IBM pentru sistemele dumneavoastră, vedeți <http://www.ibm.com/support/electronic>.

Notă: Trebuie să-i transmiteți informații furnizorului de servicii imediat ce consola HMC este instalată și configurată pentru utilizare.

Despre acest task

Pentru a transmite informațiile de service, parcurgeți pașii următori:

Procedură



1. În zona de navigare, faceți clic pe pictograma **Serviceability** și apoi selectați **Service Management**.
2. În panoul de conținut, faceți clic pe **Transmit Service Information**.
3. Efectuați taskurile din fereastra **Transmit Service Information** și faceți clic pe **OK**.

Configurarea Events Manager for Call Home

Aflați cum se configurează taskul Events Manager for Call Home. Puteți monitoriza și aproba orice date care sunt transmise de la un HMC către IBM prin acest task.

Modul Events Manager for Call Home (activat sau dezactivat) este setat folosind interfața linie de comandă HMC. Activarea taskului Events Manager for Call Home blochează în mod automat apelarea de către HMC a evenimentelor acasă atunci când acestea apar. Pentru a preveni apelarea evenimentelor fără aprobare, toate consolele HMC care rulează în acest mediu trebuie să aibă activat Events Manager for Call Home.

Pentru a activa sau a dezactiva taskul Events Manager for Call Home, rulați următoarea comandă:

```
chhmc -c emch
```

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

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

```
[--help]
```

Notă: Activând taskul Events Manager for Call Home blochează evenimentele call-home până când sunt aprobate pentru taskul call-home. Dacă dezactivați taskul Events Manager for Call Home, nu activează automat caracteristica call-home. Această setare previne orice apelare acasă neintenționată a datelor înapoi către IBM. Alegeți dintre opțiunile de comandă următoare pentru a seta configurația necesară:

- Pentru a activa taskul Events Manager for Call Home: **chhmc -c emch -s enable**
- Pentru a dezactiva taskul Events Manager for Call Home și a reactiva call-home automat: **chhmc -c emch -s disable --callhome enable**
- Pentru a dezactiva taskul Events Manager for Call Home și a nu reactiva call-home automat: **chhmc -c emch -s disable --callhome disable**

Asigurați-vă că HMC poate comunica cu alte console HMC implementate în acest mediu. Events Manager for Call Home are o funcție de conexiune test atunci când este înregistrat un HMC.

Puteți înregistra consola HMC cu Events Manager for Call Home. După ce înregistrați consola HMC, managerul de evenimente interoghează consola HMC înregistrată după evenimente care așteaptă să fie trimise prin call-home către IBM. Events Manager arată care date sunt trimise înapoi către IBM și aprobă

aceste evenimente. După aprobare, Event Manager anunță consola HMC înregistrată că poate continua cu operația call-home.

Taskul Events Manager for Call Home poate fi rulat de la orice HMC sau de la mai multe console HMC. Pentru a înregistra o consolă de gestionare cu taskul Events Manager for Call Home, efectuați pașii următori:



1. În zona de navigare, faceți clic pe pictograma **Serviceability** și apoi selectați **Events Manager for Call Home**.
2. Din panoul **Events Manager for Call Home**, faceți clic pe **Manage Consoles**.
3. Din fereastra **Manage Registered Consoles** faceți clic pe **Add Console** pentru a introduce informații pentru a înregistra o consolă de gestionare cu taskul Events Manager for Call Home.
4. Faceți clic pe **OK** pentru a efectua modificările la lista de console de gestionare înregistrate.

Notă: Events Manager for Call Home poate fi folosit cu modul manager de evenimente dezactivat. Puteți în continuare să înregistrați consola HMC și să vizualizați evenimente în managerul de evenimente, dar Events Manager nu controlează momentul în care evenimentele sunt transmise call-home.

Setarea parolelor pentru sistemul gestionat

Trebuie să setați parolele atât pentru server, cât și pentru ASM (Advanced System Management). Vedeți cum se folosește interfața HMC pentru a seta aceste parole.

Înainte de a începe

Dacă ați primit mesajul Authentication Pending, consola HMC vă promptează să setați parolele pentru sistemul gestionat.

Despre acest task

Dacă nu ați primit mesajul Authentication Pending, parcurgeți pașii următori pentru a seta parolele sistemului gestionat.

Actualizarea parolei de server

Înainte de a începe

Pentru a actualiza parola serverului, procedați în felul următor:

Procedură

1. În zona de navigare, faceți clic pe sistemul gestionat, faceți clic pe pictograma **Users and Security**



și apoi selectați **Users and Roles**.

2. Faceți clic pe **Change Password**. Se deschide fereastra Update Password.
3. Introduceți informațiile necesare și faceți clic pe **OK**.

Actualizarea parolei generale ASM (Advanced System Management)

Înainte de a începe

Notă: Parola implicită pentru ID-ul de utilizator general este general și parola implicită pentru ID-ul administrator este admin.

Pentru a actualiza parola generală ASM, procedați în felul următor:

Procedură

1. În zona de navigare a consolei HMC, selectați sistemul gestionat.
2. În zona de taskuri, faceți clic pe **Operations**.
3. Faceți clic pe **Advanced System Management (ASM)**. Se deschide fereastra Launch ASM Interface.
4. Selectați o adresă IP pentru procesorul de service și faceți clic pe **OK**. Se deschide interfața ASM.
5. În panoul de bun venit ASMI, specificați ID-ul și parola și faceți clic pe **Log In**.
6. În zona de navigare, expandați **Login Profile**.
7. Selectați **Change Password**.
8. Specificați informațiile cerute și faceți clic pe **Continue**.

Resetarea parolei de administrator ASM (Advanced System Management)

Înainte de a începe

Pentru resetarea parolei de administrator, contactați un furnizor de servicii autorizat.

Testarea conexiunii între consola HMC și sistemul gestionat

Aflați cum să verificați că sunteți conectat corespunzător la rețea.

Despre acest task

Pentru a testa rețeaua, trebuie să fiți un membru al unuia din următoarele roluri:

- Super administrator
- Reprezentant de service

Pentru a testa conexiunea între HMC și sistemul gestionat, procedați în felul următor:

Procedură

1. În zona de navigare, faceți clic pe pictograma **HMC Management**  și apoi selectați **Console Settings**.
2. În panoul de conținut, faceți clic pe **Test Network Connectivity**.
3. În fișa Ping, introduceți numele de gazdă sau adresa IP a sistemului la care doriți să vă conectați. Pentru a testa o rețea deschisă, tastați gateway-ul. Apăsați **Ping**.

Rezultate

Dacă nu ați creat încă partiții logice, nu veți putea face ping la adrese. Puteți folosi consola HMC pentru a crea partiții logice pe server. Pentru informații suplimentare, vedeți [Partiționarea logică](#).

Pentru a înțelege cum poate fi folosită consola HMC în rețea, vedeți [“Conexiunile de rețea HMC” la pagina 36](#).

Pentru informații suplimentare despre configurarea consolei HMC pentru a se conecta la o rețea, vedeți [“Configurarea HMC folosind meniurile ” la pagina 53](#).

Pași post-configurare

După ce ați instalat și configurat consola HMC, salvați datele consolei HMC după cum este necesar.

Salvarea de rezervă a datelor consolei de gestionare

Acest task realizează salvarea de rezervă (sau arhivarea) datelor stocate pe discul consolei HMC care sunt critice pentru suportul operațiilor consolei HMC.

Înainte de a începe

Sistemul de la distanță trebuie să aibă NFS (Network File System) sau ssh (Secure Shell) configurat și această rețea trebuie să fie accesibilă de la consola HMC. Pentru a realiza acest task, trebuie să opriți și să reporniți consola HMC. Folosiți doar consola HMC pentru a realiza aceste taskuri.

Despre acest task

Pentru salvarea de rezervă a unității de disc HMC pe un sistem la distanță, trebuie să fiți membru al unui dintre următoarele roluri:

- Super administrator
- Operator
- Reprezentant de service

Salvați datele HMC după ce s-au făcut modificări consolei HMC sau informațiilor asociate cu partițiile logice.

Datele consolei HMC stocate pe discul acesteia pot fi salvate pe DVD-RAM-ul sistemului local, pe un sistem la distanță, montat la sistemul de fișiere al consolei HMC (cum ar fi NFS), sau poate fi trimis într-o locație la distanță prin FTP (File Transfer Protocol).

Notă: Pentru modelul HMC 7063-CR1, puteți conecta un dispozitiv USB sau DVD extern.

Folosind consola HMC, puteți salva copii de siguranță pentru toate datele importante, cum ar :

- Fișierele cu preferințele utilizatorului
- Informațiile utilizatorului
- Fișierele de configurație-platformă a consolei HMC
- Fișierele istoric ale consolei HMC
- Actualizarea consolei HMC prin Install Corrective Service.

Pentru salvarea de rezervă a datelor de pe hard disc-ul HMC pe un sistem la distanță, finalizați pașii următori:

Procedură

1. În zona de navigare, faceți clic pe pictograma **HMC Management**  și apoi selectați **Console Managment**.
2. În panoul de conținut, faceți clic pe **Backup Management Console Data**.
3. Din fereastra **Backup Management Console Data** alegeți opțiunea de arhivare pe care doriți să o efectuați.
4. Faceți clic pe **Next**, apoi urmați instrucțiunile corespunzătoare în funcție de opțiunea pe care ați ales-o.
5. Faceți clic pe **OK** pentru a continua cu procesul de salvare de rezervă.

Actualizarea, modernizarea și migrarea codului de mașină al consolei HMC

Periodic, sunt lansate actualizări și modernizări pentru consola HMC, pentru a-i suplimenta funcționalitatea și a-i îmbunătăți caracteristicile existente. Aflați care sunt diferențele dintre actualizarea, modernizarea și migrarea codului de mașină al consolei HMC. De asemenea, aflați cum să realizați actualizarea, modernizarea sau migrarea codului de mașină al consolei HMC.

Când ați terminat cu fiecare din aceste taskuri, consola HMC repornește, dar partițiile nu.

Actualizarea codului consolei HMC

Aplică întreținerea unui nivel de consolă HMC existent

Nu necesită să realizați taskul **Salvarea de date de modernizare**

Modernizarea codului consolei HMC

Înlocuiește software-ul HMC cu o nouă ediție sau nivel de corecție al aceluiași program

Necesită să executați boot de pe mediul de recuperare

Migrarea codului consolei HMC

Mută date HMC de la o versiune de consolă HMC la alta

O migrare este un tip de modernizare.

Notă: Pentru modelul HMC 7063-CR1, puteți conecta un dispozitiv USB DVD extern.

Determinarea versiunii și ediției codului de mașină HMC

Aflați cum puteți să vizualizați versiunea și ediția codului de mașină HMC.

Despre acest task

Nivelul codului de mașină de pe HMC va determina caracteristicile disponibile, inclusiv menținerea concurentă a firmware-ului serverului și îmbunătățirile pentru modernizarea la o nouă ediție.

Pentru a vizualiza versiunea și ediția codului de mașină HMC, procedați în felul următor:

Procedură

1. În zona de navigare, faceți clic pe pictograma **HMC Management**  și apoi selectați **Console Management**.
2. În panoul de conținut, apăsați pe **Update the Hardware Management Console**.
3. În noua fereastră, vedeți și înregistrați informațiile care apar sub antetul **Current HMC Driver Information** inclusiv: nivelul de versiune, ediție, întreținere al consolei HMC, nivelul de build și versiunile de bază.

Obținerea și aplicarea actualizărilor codului de mașină pentru consola HMC cu o conexiune la internet

Aflați cum puteți să obțineți actualizările codului de mașină pentru HMC când consola HMC are o conexiune la Internet.

Despre acest task

Pentru a descărca actualizările codului de mașină pentru HMC, urmați pașii:

Pasul 1. Asigurați-vă că aveți o conexiune la Internet

Despre acest task

Pentru a descărca actualizări de la sistemul sau site-ul web de suport și service la HMC sau la server, trebuie să aveți una dintre următoarele conexiuni:

- Conectivitate SSL cu sau fără un proxy SSL
- Internet VPN

Pentru a vă asigura că aveți o conexiune la Internet, procedați în felul următor:

Procedură

1. În zona de navigare, faceți clic pe pictograma **Serviceability**  și apoi selectați **Service Management**.

2. În panoul de conținut, faceți clic pe **Manage Outbound Connectivity**.
3. Selectați fila pentru tipul de conectivitate de ieșire pe care îl alegeți pentru consola HMC (VPN prin Internet sau conectivitate SSL).

Notă: Dacă nu există o conexiune la organizația de service și suport, setați conexiunea de service înainte de a continua cu această procedură. Pentru instrucțiuni privind setarea unei conexiuni la organizația de service și suport, vedeți Setarea serverului pentru conectarea la organizația IBM de service și suport.

4. Faceți clic pe **Test**.
5. Verificați dacă testul este completat cu succes.
Dacă testul nu a fost terminat cu succes, verificați capacitatea de conectare și corectați problema înainte de a continua cu această procedură. Sau puteți obține actualizarea pe DVD.
Notă: Pentru modelul HMC 7063-CR1, puteți conecta un dispozitiv USB sau DVD extern.
6. Continuați cu [“Pasul 2. Vizualizați nivelul codului de mașină existent al consolei HMC”](#) la pagina 76.

Pasul 2. Vizualizați nivelul codului de mașină existent al consolei HMC

Despre acest task

Pentru a vizualiza nivelul existent al codului de mașină HMC, procedați în felul următor:

Procedură

1. În zona de navigare, faceți clic pe pictograma **HMC Management**  și apoi selectați **Console Management**.
2. În panoul de conținut, apăsați pe **Update the Hardware Management Console**.
3. În noua fereastră, vedeți și înregistrați informațiile care apar sub antetul Current HMC Driver Information, inclusiv: nivelul de versiune, ediție, întreținere al consolei HMC, nivelul de build și versiunile de bază.
4. Continuați cu [“Pasul 3. Vizualizați nivelurile de cod de mașină HMC disponibile”](#) la pagina 76.

Pasul 3. Vizualizați nivelurile de cod de mașină HMC disponibile

Despre acest task

Pentru a vizualiza nivelurile disponibile ale codului de mașină HMC, procedați în felul următor:

Procedură

1. De pe un calculator sau un server cu conexiune la Internet, vizitați <http://www.ibm.com/eserver/support/fixes>.
2. Selectați familia corespunzătoare în lista Product family.
3. Selectați **Hardware Management Console** în lista Product or fix type.
4. Faceți clic pe **Continue**.
Este afișat site-ul Hardware Management Console.
5. Defilați la nivelul versiunii dumneavoastră de HMC pentru a vizualiza nivelurile disponibile de HMC.
Notă: Dacă preferați, puteți lua legătura cu organizația de service și suport.
6. Continuați cu [“Pasul 4. Aplicați actualizarea codului de mașină HMC”](#) la pagina 77.

Pasul 4. Aplicați actualizarea codului de mașină HMC

Despre acest task

Pentru a aplica actualizarea codului de mașină HMC, procedați în felul următor:

Procedură

1. Înainte de a instala actualizările codului de mașină HMC, salvați pe HMC informațiile critice ale consolei.
Pentru instrucțiuni, vedeți [“Salvarea de rezervă a datelor consolei de gestionare” la pagina 73](#). Apoi continuați cu următorul pas.



2. În zona de navigare, faceți clic pe pictograma **HMC Management** și apoi selectați **Console Management**.
3. În panoul de conținut, apăsați pe **Update the Hardware Management Console**. Se deschide vrăjitorul Install Corrective Service.
4. Urmăriți instrucțiunile din vrăjitor pentru a instala actualizările.
5. Opriți și reporniți consola HMC pentru ca actualizarea să devină efectivă.
6. Faceți clic pe **Log on and launch the Hardware Management Console web application**.
7. Logați-vă la interfața consolei HMC.

Pasul 5. Verificați dacă actualizarea codului de mașină HMC s-a instalat cu succes

Despre acest task

Pentru a verifica dacă s-a instalat corect actualizarea codului de mașină HMC, procedați în felul următor::

Procedură



1. În zona de navigare, faceți clic pe pictograma **HMC Management** și apoi selectați **Console Management**.
2. În panoul de conținut, apăsați pe **Update the Hardware Management Console**.
3. În noua fereastră, vedeți și înregistrați informațiile care apar sub antetul Current HMC Driver Information, inclusiv: nivelul de versiune, ediție, întreținere al consolei HMC, nivelul de build și versiunile de bază.
4. Verificați faptul că versiunea și ediția se potrivesc cu actualizarea pe care ați instalat-o.
5. Dacă nivelul de cod afișat nu este nivelul pe care l-ați instalat, efectuați următorii pași:
 - a. Selectați conexiunea la rețea pentru consola HMC.
 - b. Încercați din nou actualizarea firmware-ului folosind o altă magazie.
 - c. Dacă problema persistă, contactați următorul nivel de suport.

Obținerea și aplicarea actualizărilor codului de mașină pentru consola HMC folosind DVD sau un server FTP

Aflați cum puteți să obțineți actualizările codului de mașină pentru HMC folosind un DVD sau un server FTP.

Despre acest task

Pentru a obține actualizările codului de mașină, urmați pașii de mai jos:

Notă: Pentru modelul HMC 7063-CR1, puteți conecta un dispozitiv USB DVD extern.

Pasul 1. Vizualizați nivelul codului de mașină existent al consolei HMC

Înainte de a începe

Pentru a vizualiza nivelul existent al codului de mașină HMC, procedați în felul următor:

Procedură

1. În zona de navigare, faceți clic pe pictograma **HMC Management**  și apoi selectați **Console Management**.
2. În panoul de conținut, apăsați pe **Update the Hardware Management Console**.
3. În noua fereastră, vedeți și înregistrați informațiile care apar sub antetul Current HMC Driver Information, inclusiv: nivelul de versiune, ediție, întreținere al consolei HMC, nivelul de build și versiunile de bază.
4. Continuați cu [“Pasul 2. Vizualizați nivelurile de cod de mașină HMC disponibile” la pagina 78.](#)

Pasul 2. Vizualizați nivelurile de cod de mașină HMC disponibile

Înainte de a începe

Pentru a vizualiza nivelurile disponibile ale codului de mașină HMC, procedați în felul următor:

Despre acest task

Procedură

1. De pe un computer sau un server cu conexiune la internet, accesați site-ul web [Fix Central](#).
 2. Defilați la nivelul versiunii dumneavoastră de HMC, pentru a vizualiza nivelurile de HMC disponibile.
- Notă:** Dacă preferați, puteți lua legătura cu organizația IBM de service și suport.
3. Continuați cu [“Pasul 3. Obțineți actualizarea codului de mașină HMC” la pagina 78.](#)

Pasul 3. Obțineți actualizarea codului de mașină HMC

Înainte de a începe

Pentru a obține actualizarea codului de mașină HMC, procedați în felul următor:

Despre acest task

Puteți să comandați actualizarea codului de mașină HMC prin site-ul web [Fix Central](#), să contactați organizația de service și suport sau să o descărcați de pe un server FTP.

Comandarea actualizării codului de mașină al consolei HMC prin site-ul web [Fix Central](#)

1. De pe un computer sau un server cu conexiune la internet, accesați site-ul web [Fix Central](#).
2. Sub Supported HMC products, selectați cel mai recent nivel de HMC.
3. Defilați la zona File names / Package și localizați actualizarea pe care vreți să o comandați.
4. În coloana Order, selectați **Go**.
5. Faceți clic pe **Continue** pentru a semna cu ID-ul dumneavoastră IBM.
6. Urmăriți prompturile de pe ecran pentru a vă lansa comanda de achiziție.

Descărcarea actualizării codului de mașină HMC pe un mediu de stocare amovibil

1. De pe un computer sau un server cu conexiune la internet, accesați site-ul web [Fix Central](#).
2. Sub Supported HMC products, selectați cel mai recent nivel de HMC.
3. Defilați în jos la zona File names / Package și localizați actualizarea pe care doriți să o descărcați.
4. Faceți clic pe actualizarea pe care doriți să o descărcați.
5. Acceptați acordul de licență și salvați actualizarea pe mediul dumneavoastră de stocare amovibil.

Ce se face în continuare

După ce ați terminat, continuați cu [“Pasul 4. Aplicați actualizarea codului de mașină HMC”](#) la pagina 79.

Pasul 4. Aplicați actualizarea codului de mașină HMC

Înainte de a începe

Pentru a aplica actualizarea codului de mașină HMC, procedați în felul următor:

Procedură

1. Înainte de a instala actualizările codului de mașină HMC, faceți o copie de rezervă cu datele HMC. Pentru informații suplimentare, vedeți [“Salvarea de rezervă a datelor consolei de gestionare”](#) la pagina 73.
2. Dacă ați obținut sau ați creat actualizarea pe DVD-RAM, introduceți-l în unitatea DVD de pe HMC. Dacă ați obținut sau ați creat actualizările pe un dispozitiv de memorie USB, introduceți dispozitivul de memorie.
3. Înainte de a instala actualizările codului de mașină HMC, salvați pe HMC informațiile critice ale consolei.
Pentru instrucțiuni, vedeți [“Salvarea de rezervă a datelor consolei de gestionare”](#) la pagina 73. Apoi continuați cu următorul pas.
4. În zona de navigare, faceți clic pe pictograma **HMC Management**  și apoi selectați **Console Management**.
5. În panoul de conținut, apăsați pe **Update the Hardware Management Console**. Se deschide vrăjitorul Install Corrective Service.
6. Urmăriți instrucțiunile din vrăjitor pentru a instala actualizările.
7. Pentru ca actualizarea să devină efectivă, opriți și reporniți consola HMC și apoi logați-vă înapoi.
8. Continuați cu [“Pasul 5. Verificați dacă actualizarea codului de mașină HMC s-a instalat cu succes”](#) la pagina 79.

Pasul 5. Verificați dacă actualizarea codului de mașină HMC s-a instalat cu succes

Înainte de a începe

Pentru a verifica dacă s-a instalat cu succes actualizarea codului de mașină HMC, procedați în felul următor:

Procedură

1. În zona de navigare, faceți clic pe pictograma **HMC Management**  și apoi selectați **Console Management**.
2. În panoul de conținut, apăsați pe **Update the Hardware Management Console**.

3. În noua fereastră, vedeți și înregistrați informațiile care apar sub antetul Current HMC Driver Information, inclusiv: nivelul de versiune, ediție, întreținere al consolei HMC, nivelul de build și versiunile de bază.
4. Verificați faptul că versiunea și ediția se potrivesc cu actualizarea pe care ați instalat-o.
5. Dacă nivelul de cod afișat nu este nivelul pe care l-ați instalat, efectuați următorii pași:
 - a. Reîncercați actualizarea codului de mașină. Dacă ați creat un DVD pentru această procedură, folosiți un mediu de stocare nou.
 - b. Dacă problema persistă, contactați următorul nivel de suport.

Modernizarea software-ului HMC

Aflați cum modernizați software-ul HMC de la o ediție la următoarea păstrând datele de configurare ale consolei HMC.

Despre acest task

Pentru a moderniza codul de mașină pe o consolă HMC, urmați pașii:

Notă: Pentru modelele HMC 7063-CR1 și 7063-CR2, puteți conecta o unitate DVD USB externă.

Pasul 1. Obțineți modernizarea

Despre acest task

Puteți comanda actualizarea codului de mașină HMC prin site-ul web [Fix Central](#).

Pentru a obține actualizarea prin site-ul web [Fix Central](#), parcurgeți pașii următori:

Procedură

1. De la un computer sau server cu o conexiune de Internet, mergeți la site-ul web pentru Hardware Management Console la <http://www-933.ibm.com/support/fixcentral/>.
2. Faceți clic pe **Continue**.
Este afișat site-ul Hardware Management Console.
3. Navigați la versiunea de consolă HMC la care doriți să faceți modernizarea.
4. Localizați secțiunea de descărcare și comandare.

Notă: Dacă nu aveți acces la Internet, luați legătura cu organizația IBM de service și suport pentru a comanda modernizarea pe DVD.

5. Urmăriți prompturile de pe ecran pentru a vă lansa comanda de achiziție.
6. După ce aveți actualizarea, continuați cu "[Pasul 2. Vizualizați nivelul codului de mașină existent al consolei HMC](#)" la pagina 80.

Pasul 2. Vizualizați nivelul codului de mașină existent al consolei HMC

Despre acest task

Pentru a determina nivelul existent al codului de mașină pe o consolă HMC, urmați acești pași:

Procedură

1. În zona de navigare, faceți clic pe pictograma **HMC Management**  și apoi selectați **Console Management**. În zona de navigare, faceți clic pe **Updates**.
2. În panoul de conținut, apăsați pe **Update the Hardware Management Console**.

3. În noua fereastră, vedeți și înregistrați informațiile care apar sub antetul Current HMC Driver, inclusiv versiunea și ediția consolei HMC, nivelul de întreținere, nivelul de build și versiunile de bază.
4. Continuați cu [“Pasul 3. Faceți o copie de rezervă cu datele de profil ale sistemului gestionat”](#) la pagina 81.

Pasul 3. Faceți o copie de rezervă cu datele de profil ale sistemului gestionat

Despre acest task

Pentru a realiza o copie de rezervă cu datele de profil ale sistemului gestionat, procedați în felul următor:

Procedură

1. Selectați sistemul pe care vreți să salvați datele de profil.
2. Faceți clic pe **Actions > View All Actions > Legacy > Manage Partition Data > Backup**.
3. Tastați un nume pentru fișierul cu copia de rezervă și notați aceste informații.
4. Faceți clic pe **OK**.
5. Repetați acești pași pentru fiecare sistem.
6. Continuați cu [“Pasul 4. Faceți o copie de rezervă cu datele consolei HMC”](#) la pagina 81.

Pasul 4. Faceți o copie de rezervă cu datele consolei HMC

Despre acest task

Salvați datele consolei HMC înainte de a instala o nouă ediție de software HMC, astfel încât să poată fi restaurate nivelurile anterioare în eventualitatea apariției unei probleme în timpul modernizării software-ului. Nu folosiți aceste date critice ale consolei după modernizarea cu succes la o nouă versiune de software HMC.

Notă: Pentru salvarea pe mediul de stocare amovibil, trebuie să aveți disponibil mediul respectiv.

Pentru a salva datele HMC, procedați în felul următor:

Procedură

1. Dacă intenționați să faceți salvarea de rezervă pe un mediu de stocare, parcurgeți pașii următori pentru a formata mediul:
 - a. Introduceți mediul de stocare în unitate.
 - b. În zona de navigare, faceți clic pe pictograma **Serviceability**  și apoi selectați **Service Management**.
 - c. În panoul de conținut, faceți clic pe **Format Media**.
 - d. Selectați tipul de mediu de stocare.
 - e. Selectați tipul de format.
 - f. Faceți clic pe **OK**.
2. În zona de navigare, faceți clic pe pictograma **HMC Management**  și apoi selectați **Console Management**.
3. În panoul de conținut, faceți clic pe **Backup Management Console Data**.
Se deschide fereastra **Backup Management Console Data**.
4. Selectați o opțiune de arhivare.

Puteți salva pe mediul de stocare de pe sistemul local, pe un sistem de la distanță montat pe sistemul de fișiere HMC (de exemplu, NFS) sau puteți trimite copia de rezervă la un site de la distanță folosind FTP (File Transfer Protocol).

- Pentru a salva la un sistem local, alegeți **Back up to media on local system** și urmați instrucțiunile.
- Pentru a salva la un sistem de la distanță, alegeți **Back up to mounted remote system** și urmați instrucțiunile.
- Pentru a salva la un site FTP, alegeți **Send back up critical data to remote site** și urmați instrucțiunile.

5. Continuați cu [“Pasul 5. Înregistrați informațiile curente de configurare a consolei HMC”](#) la pagina 82.

Pasul 5. Înregistrați informațiile curente de configurare a consolei HMC

Despre acest task

Înainte de a moderniza la o nouă versiune de software HMC, ca o măsură de precauție, înregistrați informațiile de configurație HMC.

Pentru a înregistra configurația curentă a consolei HMC, procedați în felul următor:

Procedură

1. Selectați un sistem gestionat sau orice partiții pentru care doriți să înregistrați informațiile de configurație HMC.
2. Din blocul de meniuri, selectați **Actions > Schedule Operations**.
Sunt afișate toate operațiile planificate pentru ținta selectată.
3. Selectați **Sort > By object**.
4. Selectați fiecare obiect și înregistrați următoarele detalii:
 - Numele obiectului
 - Data programării
 - Timpul de funcționare (afișat în format de 24 de ore)
 - Repetitiv (dacă este Da, parcurgeți pașii următori):
 - a. Selectați **View > Schedule Details**.
 - b. Înregistrați informațiile de interval.
 - c. Închideți fereastra de planificare operații.
 - d. Repetați pentru fiecare operație planificată.
5. Închideți fereastra **Customize Scheduled Operations**.
6. Continuați cu [“Pasul 6. Înregistrați starea comenzii la distanță”](#) la pagina 82.

Pasul 6. Înregistrați starea comenzii la distanță

Despre acest task

Pentru a înregistra starea comenzii la distanță, procedați în felul următor:

Procedură

1. În zona de navigare, faceți clic pe pictograma **Users and Security**  și apoi selectați **Systems and Console Security**.
2. În panoul de conținut, faceți clic pe **Enable Remote Command Execution**.
3. Notați dacă este selectată caseta de bifare **Enable remote command execution using the ssh facility**.

4. Faceți clic pe **Cancel**.
5. Continuați cu [“Pasul 7. Salvați datele de modernizare”](#) la pagina 83.

Pasul 7. Salvați datele de modernizare

Despre acest task

Puteți salva configurația HMC curentă pe o partiție de disc desemnată pe consola HMC sau pe mediul de stocare local. Salvați datele de modernizare numai cu puțin timp înainte de a moderniza software-ul HMC la o nouă ediție. Această acțiune vă permite să restaurați setările de configurație HMC după modernizare.

Notă: Este permis doar un nivel de date copie de rezervă. De fiecare dată când salvați date de modernizare, nivelul anterior este suprascris.

Pentru a salva datele de modernizare, procedați în felul următor:

Procedură

1. În zona de navigare, faceți clic pe pictograma **HMC Management**  și apoi selectați **Console Management**.
2. În panoul de conținut, faceți clic pe **Save Upgrade Data**. Se deschide vrăjitorul **Save Upgrade Data**.
3. Selectați mediul de stocare unde vreți să salvați datele de modernizare. Dacă ați ales să salvați pe un mediu amovibil, inserați mediul acum. Faceți clic pe **Next**.
4. Faceți clic pe **Finish**.
5. Așteptați ca taskul să se finalizeze.
Dacă taskul Save Upgrade Data eșuează, contactați următorul nivel de suport înainte de a continua.
Notă: Dacă taskul de salvare a datelor de modernizare eșuează, nu continuați procesul de modernizare.
6. Faceți clic pe **OK**.
7. Continuați cu [“Pasul 8. Modernizați software-ul HMC”](#) la pagina 83.

Pasul 8. Modernizați software-ul HMC

Despre acest task

Pentru a moderniza software-ul HMC, reporniți sistemul cu mediul de stocare amovibil în unitatea DVD.

Procedură

1. Introduceți mediul de stocare HMC Product Installation în unitatea DVD.
2. În zona de navigare, faceți clic pe pictograma **HMC Management**  și apoi selectați **Console Management**.
3. În panoul de conținut, selectați **Shutdown or Restart the Management Console**.
4. Asigurați-vă că este selectată opțiunea **Restart the HMC**.
5. Faceți clic pe **OK**.
HMC repornește și informațiile de sistem defilează în fereastră.
6. Selectați **Upgrade** și apăsați **Next**.
7. Alegeți din următoarele opțiuni:
 - Dacă ați salvat date de modernizare în timpul taskului anterior, continuați cu pasul următor.
 - Dacă nu ați salvat date de modernizare anterior în această procedură, trebuie să salvați datele de modernizare acum înainte de a continua.

8. Selectați **Upgrade from media** și apăsați **Next**.
9. Confirmați setările și apăsați **Finish**.
10. Urmați prompturile.

Notă:

- Dacă ecranul devine gol, apăsați bara de spațiu pentru a vizualiza informațiile.
 - Pentru primul DVD, instalarea poate dura aproximativ 20 de minute.
11. La promptul de logare, logați-vă folosind ID-ul de utilizator și parola.
Instalarea codului HMC este finalizată.
 12. Continuați cu [“Pasul 9. Verificați instalarea cu succes a modernizării codului de mașină HMC” la pagina 84.](#)

Pasul 9. Verificați instalarea cu succes a modernizării codului de mașină HMC

Despre acest task

Pentru a verifica dacă s-a instalat cu succes modernizarea consolei HMC, procedați în felul următor:

Procedură

1. În zona de navigare, faceți clic pe pictograma **HMC Management**  și apoi selectați **Console Management**.
2. În panoul de conținut, apăsați pe **Update the Hardware Management Console**.
3. În noua fereastră, vedeți și înregistrați informațiile care apar sub antetul Current HMC Driver, inclusiv versiunea și ediția consolei HMC, nivelul de întreținere, nivelul de build și versiunile de bază.
4. Verificați faptul că versiunea și ediția se potrivesc cu actualizarea pe care ați instalat-o.
5. Dacă nivelul de cod afișat nu este nivelul pe care l-ați instalat, reîncercați taskul de modernizare folosind un nou DVD. Dacă problema persistă, contactați următorul nivel de suport.

Modernizarea HMC dintr-o locație la distanță utilizând imagini de modernizare rețea

Aflați cum modernizați software-ul pe un HMC dintr-o locație la distanță utilizând imagini de modernizare rețea.

Despre acest task

Aflați cum modernizați software-ul pe un HMC dintr-o locație la distanță utilizând imagini de modernizare rețea.

Procedură

1. De la un calculator sau server cu o conexiune la Internet, accesați site-ul web [Website pentru suport și descărcări Hardware Management Console](http://www14.software.ibm.com/webapp/set2/sas/f/hmcl/home.html)(<http://www14.software.ibm.com/webapp/set2/sas/f/hmcl/home.html>).
2. Descărcați imaginile corespunzătoare de rețea HMC V9 și salvați-le pe un server FTP.
Nu puteți descărca aceste fișiere direct la HMC. Trebuie să descărcați fișierele de imagini pe un server care acceptă cereri FTP.
3. Asigurați-vă că descărcați fișierele următoare:
 - img2a
 - img3a
 - base.img

- disk1.img
 - hmcnetworkfiles.sum
- Salvați datele de modernizare pe un HMC. Rulați următoarele comenzi pentru a salva datele de modernizare:
 - Pentru a salva date și pe DVD și pe HDD, executați comenzile următoare:


```
mount /media/cdrom
saveupgdata -r diskdvd
```
 - Pentru a salva date pe HDD, executați comanda următoare:


```
saveupgdata -r disk
```
 - Copiați fișierele de modernizare la partiția de disc resetabilă pe HMC. Rulați comanda **getupgfiles** pentru a copia fișierele.
Exemplu: **getupgfiles -h <ftp server> -u <user id> -d <remote directory>**
unde,
 - ftp server** este numele gazdă sau adresa IP a serverului FTP unde descărcați imaginile de rețea HMC.
 - user id** este un id de utilizator valid de pe serverul FTP. Dacă nu specificați parola cu argumentul **-passwd**, veți fi promptat pentru o parolă.
 - remote directory** este directorul de pe serverul dumneavoastră FTP unde sunt salvate imaginile de rețea HMC.
 - Resetați consola HMC pentru a moderniza codul copiat la partiția resetabilă de disc. Rulați **chhmc -c altdiskboot -s enable --mode upgrade** pentru a reporni sistemul HMC.
 - Resetați sistemul HMC și începeți modernizarea. Rulați comanda **hmcshutdown -r -t now** pentru a începe modernizarea.

Securizarea consolei HMC

Aflați cum puteți îmbunătăți securitatea consolei HMC (Hardware Management Console) pe baza standardelor dumneavoastră de securitate corporative.

Configurația implicită a consolei HMC asigură un nivel înalt de securitate pentru majoritatea utilizatorilor din întreținere. Cu Hardware Management Console (HMC) Versiunea 8.4.0 sau ulterioară, puteți îmbunătăți securitatea consolei HMC pe baza standardelor dumneavoastră de securitate corporative. Pentru a îmbunătăți securitatea consolei HMC, trebuie să setați HMC la nivelul minim de securitate, Nivelul 1. În funcție de mediul dumneavoastră și cerințele de securitate corporative, puteți alege securitatea Nivelul 2 și Nivelul 3.

Notă: Înainte de a modifica nivelul de securitate, consultați-vă cu echipa responsabilă pentru conformitatea cu securitatea corporativă.

Securitatea Nivelul 1

Pentru a securiza consola HMC (securitatea de nivelul 1), finalizați pașii următori:

- Schimbați parola predefinită pentru utilizatorul **hscroot** implicit. Pentru informații suplimentare despre politica privind parolele, consultați [“Politica de parolă îmbunătățită”](#) la pagina 87.
- Dacă HMC nu aparține unui mediu securizat fizic, setați parola grub rulând următoarea comandă:


```
chhmc -c grubpasswd -s enable --passwd <new grub password>
```
- Dacă ați configurat Integrated Management Module (IMM) pe HMC, setați o parolă IMM puternică.
- Setați o parolă puternică pentru utilizatorul *admin* și utilizatorii generali pe toate serverele.
- Actualizați HMC cu cele mai recente corecții pentru securitate. Pentru informații suplimentare despre corecțiile pentru securitate, vedeți [IBM Fix Central](#).

Securitatea Nivelul 2

Dacă aveți mai mulți utilizatori, finalizați următorii pași pentru a îmbunătăți securitatea pentru HMC:

1. Creați un cont pentru fiecare utilizator de pe HMC și alocați utilizatorilor rolurile și resursele necesare. Pentru informații suplimentare despre diversele roluri din HMC, consultați [Taskurile HMC, rolurile de utilizator, ID-urile și comenzile asociate](#).

Notă: Aveți grijă să alocați utilizatorilor creați pe HMC numai resursele și rolurile necesare. De asemenea, dacă este necesar, puteți să creați roluri personalizate.

2. Activați replicarea datelor de utilizator între diferitele console HMC. Replicarea datelor de utilizator poate fi realizată în modul Master-Slave sau Peer-Peer. Pentru informații suplimentare despre replicarea datelor de utilizator, consultați [Gestionarea replicării datelor](#).
3. Importați un certificat care este semnat de către Autoritatea de certificare.

Securitatea Nivelul 3

Dacă aveți mai multe console HMC și mai mulți administratori de sistem, finalizați următorii pași pentru a îmbunătăți securitatea pentru HMC:

1. Folosiți autentificarea centralizată, cum ar fi Lightweight Directory Access Protocol (LDAP) sau Kerberos. Pentru informații suplimentare despre configurarea LDAP, consultați [How to Configure LDAP on HMC](#).
2. Activați replicarea datelor de utilizator între diferitele console HMC.
3. Asigurați-vă că HMC este în [modul NIST SP 800-131A](#), astfel ca HMC să utilizeze numai cifruri puternice.
4. Blocați porturile care nu sunt necesare în firewall. Pentru informații despre porturile HMC care pot fi utilizate, consultați următorul tabel:

Tabela 32. Portul folosit de către utilizator pentru interacțiunea cu HMC				
Port	Descriere	Tip	Versiune protocol (modul implicit)	Versiune protocol (modul NIST)
22	Open SSH	TCP	SSH v3	SSH v3
123	NTP	UDP	NTP	NTP
161	SNMP Agent	UDP	SNMP v3	SNMP v3
162	SNMP Trap	UDP	SNMP v3	SNMP v3
427	SLP	UDP	-	-
443	GUI HMC și API REST	TCP	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)
657	RMC	TCP/UDP	RSCT (text simplu + hash și semn)	RSCT (text simplu + hash și semn)
2300	Terminal 5250 pentru IBM i	TCP	Text simplu	Text simplu
2301	Terminal securizat 5250 pentru IBM i	TCP	TLS 1.2	TLS 1.2
5989	CIM (port moștenire, nefuncțional)	TCP	Nefuncțional	Nefuncțional

Tabela 32. Portul folosit de către utilizator pentru interacțiunea cu HMC (continuare)				
Port	Descriere	Tip	Versiune protocol (modul implicit)	Versiune protocol (modul NIST)
9900	FCS: Descoperire HMC-HMC	UDP	FCS	FCS
9920	FCS: Comunicație HMC-HMC	TCP	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)
9960	Aplet VTerm în GUI	TCP	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)
12443	API REST HMC (port moștenit)	TCP	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)
12347	Domeniu peer RSCT	UDP	RSCT (text simplu + hash și semn)	RSCT (text simplu + hash și semn)
12348	Domeniu peer RSCT	UDP	RSCT (text simplu + hash și semn)	RSCT (text simplu + hash și semn)

Note:

- Trebuie să utilizați numai SSH (portul 22), HTTPS (portul 443 și portul 12443), terminal securizate 5250 pentru IBM i (portul 2301) și VTerm (portul 9960) expuse la un intranet. Toate celelalte porturi trebuie să fie utilizate într-o rețea privată sau izolată. Puteți folosi un port Ethernet separat și VLAN pentru RMC (Resource Monitoring and Control) (portul 657), FCS (portul 9900 și portul 9920) și domeniu peer RSCT (portul 12347 și portul 12348).
- Porturile listate în comanda **netstat** sunt utilizate numai pentru procesele interne.

Politica de parolă îmbunătățită

Puteți impune cerințe privind parolele pentru utilizatorii autentificați local, folosind Hardware Management Console (HMC). Funcția de politică de parolă îmbunătățită permite ca administratorul de sistem să seteze restricții pentru parole. Politica de parolă îmbunătățită se aplică sistemelor în care este instalată o consolă HMC.

Administratorii de sistem pot utiliza politica de parolă îmbunătățită pentru a defini o politică de parolă unică pentru toți utilizatorii. HMC furnizează o politică de parolă de securitate medie, ce poate fi activată de administratorii de sistem pentru a seta restricții pentru parole. De asemenea, administratorul de sistem poate decide activarea politicii de securitate medie sau a unei politici noi, definite de utilizator. Politica de parolă de securitate medie HMC nu poate fi înlăturată de pe sistem. Următorul tabel prezintă atributele politicii de securitate medie și valorile implicite.

Tabela 33. Atributele de parolă pentru politica de parolă de securitate medie HMC		
Atribut	Descriere	Valoare implicită
min_pwage	Numărul minim de zile în care o parolă trebuie să rămână activă.	1
pwage	Numărul maxim de zile în care o parolă poate să rămână activă.	180
min_length	Lungimea minimă a unei parole.	8
hist_size	Numărul de parole salvate anterior care nu pot fi reutilizate.	10

Tabela 33. Atributele de parolă pentru politica de parolă de securitate medie HMC (continuare)

Atribut	Descriere	Valoare implicită
warn_pwage	Când parola este pe cale să expire, numărul de zile înainte de care un utilizator este avertizat că parola este pe cale să expire.	7
min_digits	Numărul minim de cifre care trebuie să fie utilizate în parolă.	Fără
min_uppercase	Numărul minim de caractere literă mare.	1
min_lowercase	Numărul minim de caractere literă mică.	6
min_special_chars	Numărul minim de caractere speciale care trebuie să fie utilizate în parolă.	Fără

Luați în considerare următoarele articole privind politica de parolă de securitate medie HMC:

- Politica nu se aplică pentru ID-urile de utilizator **hscroot**, **hscpe** și **root**.
- Politica afectează numai utilizatorii autentificați local care sunt gestionați de HMC și politica nu poate fi impusă pentru utilizatorii LDAP sau Kerberos.
- Politica de parolă de securitate medie HMC și politica definită de utilizator le permit administratorilor de sistem să seteze restricții pentru reutilizarea parolelor.
- Politica de parolă de securitate medie HMC este numai-citire și atributele politici de parolă de securitate medie HMC nu pot fi modificate. Puteți crea o politică de parolă nouă, definită de utilizator, pentru a seta restricții pentru parole.

Puteți folosi următoarele comenzi pentru a configura politica de parolă de securitate medie HMC:

mkpwdpolicy

Importă politica de parolă dintr-un fișier, care conține toți parametrii, sau creează o politică de parolă.

lspwdpolicy

Listează toate profilurile de politică de parolă disponibile și caută parametri specifici. De asemenea, puteți vizualiza politica de parolă care este activă în acel moment.

rmpwdpolicy

Înlătură o politică de parolă inactivă existentă.

Notă: Nu puteți înlătura o politică de securitate medie activă și politica de parolă numai-citire implicită.

chpwdpolicy

Modifică parametrii unei politici de parolă inactive.

Profilurile de securitate: GDPR (Global Data Protection Regulation) și PCI-DSS (Payment Card Industry Data Security Standard)

Aflați cum tratează Hardware Management Console (HMC) informațiile confidențiale ale utilizatorilor.

Hardware Management Console (HMC) este un dispozitiv închis, care nu stochează date privind deținătorul cardului. Ca urmare, pentru HMC se aplică numai un subset al cerințelor și procedurilor de evaluare a securității IT definite de PCI-DSS. Pe HMC poate fi instalat numai cod de încredere distribuit de IBM. Când este descoperită o vulnerabilitate prin [procesul PSIRT IBM](#), sunt publicate corecții interimare. Cerințele și recomandări includ următoarele articole:

Întrebări despre GDPR

Tabela 34. Întrebări despre GDPR . Acest tabel conține informații privind întrebările referitoare la GDPR.	
Întrebări	Răspunsuri
Ce fel de date sunt stocate în HMC?	HMC stochează informațiile de configurare ale hardware-ului Power, virtualizarea PowerVM și informațiile indicilor de măsurare a performanței.
HMC procesează date personale?	Puteți furniza informații de contact pentru funcția de apelare acasă (call home). Furnizarea informațiilor de contact pentru funcția de apelare acasă este opțională.
Ce conturi predefinite sunt utilizate pentru administrarea de sistem HMC?	Utilizatorul administrator de sistem folosește numele de utilizator <i>hscroot</i> .
Conturile din HMC se referă la o anumită persoană?	Nu.
Este obligatoriu să fie furnizate date cu caracter personal în HMC?	Nu. Nu trebuie să furnizați informații ce reprezintă date personale. Furnizarea acestor informații este opțională.
Fișierul istoric HMC conține informații ce reprezintă date personale?	Nu.
Este posibilă ștergerea completă și permanentă a datelor personale?	Da. Anulați configurația funcției de apelare acasă (call home).

Întrebări despre PCI-DSS

Tabela 35. Întrebări despre PCI-DSS . Acest tabel conține informații privind întrebările referitoare la PCI-DSS	
Întrebări	Răspunsuri
Cum se instalează și se întreține o configurație de firewall pentru a proteja datele deținătorului de card?	HMC nu stochează și nu accesează date ale deținătorului de card. Dar HMC are o configurație de firewall și utilizatorul poate controla și activa porturi specifice.
Pot folosi valoarea implicită de la furnizor pentru parolele de sistem și alți parametri de securitate?	Înainte de a instala un sistem în rețea, modificați toate parolele predefinite ale utilizatorului <i>hscroot</i> .
Cum protejează HMC datele stocate ale deținătorului de card?	HMC nu stochează și nu accesează date ale deținătorului de card.
Cum criptează HMC datele deținătorului de card când acestea sunt transmise prin rețele publice?	HMC nu stochează și nu accesează date ale deținătorului de card.
Cum se utilizează și cum se actualizează cu regularitate programele antivirus?	HMC este un dispozitiv închis. Ca urmare, malware-ul nu poate infecta consola HMC.
Cum se dezvoltă și se mențin în siguranță sistemele și aplicațiile?	Trebuie să instalați manual patch-urile necesare pe sistemul dumneavoastră, de pe site-ul web IBM Fix Central . Pe HMC poate fi instalat numai cod de încredere distribuit de IBM.
HMC restricționează accesul la datele deținătorului de card?	HMC nu stochează și nu accesează date ale deținătorului de card.

Tabela 35. Întrebări despre PCI-DSS . Acest tabel conține informații privind întrebările referitoare la PCI-DSS (continuare)

Întrebări	Răspunsuri
Cum poate fi atribuit un ID unic fiecărei persoane care are acces la calculator?	Pentru a implementa această cerință, trebuie să vă asigurați că nu există ID-uri comune și să respectați politicile privind parola.
Cum poate fi restricționat accesul fizic la datele deținătorului de card?	HMC nu stochează și nu accesează date ale deținătorului de card.
Cum poate fi urmărit și monitorizat accesul la resursele de rețea și datele deținătorului de card?	HMC nu stochează și nu accesează date ale deținătorului de card.
Cum testează HMC securitatea sistemului și proceselor?	Sunt folosite unelte de scanare pentru a rula scanări de securitate pentru toate versiunile de consolă HMC. Uneltele de scanare includ: <i>Qualys</i> , <i>Nessus</i> , <i>testssl</i> , <i>ssllscan</i> și <i>ASoC</i> .
Cum poate fi menținută o politică de securitate care să includă securitatea informațiilor pentru angajați și contractori?	Administratorul de sistem dezactivează logările de utilizator de la distanță, activează logarea de utilizator în funcție de necesități și dezactivează logarea de utilizator atunci când nu mai este necesar accesul.

Rezolvarea problemelor comune în timpul securizării HMC

Aflați cum puteți rezolva unele probleme care ar putea apărea în timp ce securizați HMC.

Cum se securizează conexiunea între HMC (Hardware Management Console) și sistem?

Consola HMC se conectează la sistem prin FSP (Flexible Service Processor). Este utilizat un protocol proprietate, numit protocolul Network Client (NETC), pentru a gestiona atât FSP, cât și hipervizorul Power. Următorul tabel prezintă porturile care sunt utilizate de către HMC:

Tabela 36. Porturile de pe FSP care sunt utilizate pentru a interacționa cu HMC

Port pe FSP	Descriere	Versiune protocol (modul implicit)	Versiune protocol (modul NIST)
443	Advanced System Management Interface	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)
30000	NETC	NETC (TLS 1.2). Se repliază la SSLv3 pentru suport în cazul unui firmware mai vechi.	NETC (TLS 1.2)
30001	VTerm	NETC (TLS 1.2). Se repliază la SSLv3 pentru suport în cazul unui firmware mai vechi.	NETC (TLS 1.2)

Cum se blochează HMC?

Dacă vreți să îmbunătățiți securitatea pentru infrastructură, puteți să utilizați un dispozitiv IPS (Intrusion Prevention System) sau să plasați toate consolele HMC și serverele IBM Power Systems în spatele unui firewall. De asemenea, puteți dezactiva serviciile de rețea pe HMC, dacă nu o folosiți la distanță sau dacă vreți să securizați consola HMC. Pentru a dezactiva serviciile de rețea pe HMC, finalizați pașii următori:

1. Dezactivați execuția comenzilor la distanță folosind portul SSH.
2. Dezactivați terminalul virtual la distanță (portul VTerm).
3. Dezactivați accesul web la distanță (interfața grafică de utilizator HMC și API-ul REST).
4. Blocați porturile din firewall folosind setările de rețea HMC pentru fiecare port Ethernet configurat.

Cum se setează HMC în modul conformitate NIST SP 800-131A?

Cu HMC Versiunea 8.1.0 sau ulterioară, când setați consola HMC în modul conformitate, sunt suportate numai cifruri puternice, listate de [NIST SP 800-131A](#). Este posibil să nu vă puteți conecta la servere Power Systems mai vechi, cum ar fi serverele POWER5, care nu suportă Transport Layer Security (TLS 1.2). Pentru informații suplimentare despre schimbarea modului de securitate, consultați [Modul HMC V8R8 NIST](#).

Cum se vizualizează și se schimbă cifrurile utilizate de HMC?

Cu HMC Versiunea 8.1.0 sau ulterioară, consola HMC are inclus suport pentru seturi de cifruri mai sigure, care sunt definite în NIST 800-131A. Cifrurile care sunt utilizate în modul implicit sunt puternice. Pentru informații suplimentare despre cifrurile de criptare utilizate de HMC, rulați comanda **lshmcencr**. Dacă standardele dumneavoastră corporative necesită utilizarea unui alt set de cifruri, rulați comanda **chhmcencr** pentru a schimba cifrurile de criptare.

Pentru a lista cifrurile utilizate de HMC pentru a cripta parola de utilizator, rulați comanda următoare:

```
lshmcencr -c passwd -t c
```

Pentru a lista cifrurile de criptare utilizate de interfața de utilizator web HMC și API-ul REST, rulați comanda următoare:

```
lshmcencr -c webui -t c
```

Pentru a lista cifrurile de criptare și algoritmul MAC utilizate de interfața SSH HMC, rulați comanda următoare:

```
lshmcencr -c ssh -t c
```

```
lshmcencr -c sshmac -t c
```

Cum se verifică puterea certificatului pe HMC?

CertIFICATELE auto-semnate pe HMC utilizează SHA256 cu criptarea RSA pe 2048 de biți, care este puternică. Dacă folosiți certificate semnate de CA, asigurați-vă că nu este utilizată criptarea pe 1024 de biți, care este slabă. Pot fi folosite următoarele certificate pentru HMC:

- Certificatul semnat de CA poate fi folosit pentru interfața grafică de utilizator HMC și API-ul REST (porturile 443 și 12443).
- Portul 9920 este folosit pentru comunicația HMC la HMC. Nu puteți înlocui acest certificat cu un certificat propriu.

Cum se alege între un certificat auto-semnat (implicit) și un certificat semnat de CA?

HMC generează automat un certificat în timpul instalării. Însă puteți să generați o cerere CSR (Certificate Signing Request) de pe HMC și să obțineți un certificat nou, eliberat de o Autoritate de certificare. Apoi puteți să importați acest certificat în HMC. Asigurați-vă că obțineți și un nume de domeniu pentru HMC. Pentru mai multe detalii despre gestionarea certificatelor în HMC, consultați [Gestionarea certificatelor](#).

Cum se auditează HMC?

Auditarea consolelor HMC este axată pe cifrurile configurate și activitatea diversilor utilizatori HMC. Folosiți următoarele comenzi pentru a vizualiza activitatea diferiților utilizatori HMC:

Tabela 37. Cifrurile utilizate de HMC	
Scop	Comandă
Criptare parolă (setări globale)	<code>lshmcencr -c passwd -t c</code>
Criptare parolă pentru fiecare utilizator	<code>lshmcusr -Fname:password_encryption</code>
Cifruri SSH	<code>lshmcencr -c ssh -t c</code>
SSH MAC	<code>lshmcencr -c sshmac -t c</code>
Cifru utilizat pentru interfața grafică de utilizator HMC și API-ul REST	<code>lshmcencr -c webui -t c</code>

Folosiți următoarele comenzi pentru a monitoriza informațiile despre diverse evenimente de consolă și de service privind utilizările în HMC:

Tabela 38. Comenzile pentru vizualizarea informațiilor despre utilizatorii logați și evenimentele de consolă sau de service din HMC	
Informații	Comandă
Utilizatori GUI	<code>lslogon -r webui -u</code>
Taskuri GUI	<code>lslogon -r webui -t</code>
Utilizatori CLI	<code>lslogon -r ssh -u</code>
Taskuri CLI	<code>lslogon -r ssh -t</code>
Operații pe HMC	<code>lssvcevents -t console -d <number of days></code>
Operații pe sistem	<code>lssvcevents -t hardware -m <managed system> -d <number of days></code>

Monitorizare centralizată a evenimentelor pentru HMC: Dacă aveți multe console HMC, setați fișierul `rsyslog` pentru colectarea tuturor datelor privind utilizarea.

Cum corectează IBM vulnerabilitățile de securitate ale consolei HMC?

Pentru a răspunde în cazul incidentelor privind securitatea, IBM aplică un proces numit IBM Product Security Incident Response Team (PSIRT). IBM Product Security Incident Response Team (PSIRT) este o echipă globală care gestionează primirea, investigarea și coordonarea internă a informațiilor privind vulnerabilitățile de securitate legate de ofertele IBM. Componentele Open Source și IBM livrate cu HMC sunt monitorizate și analizate în mod activ. IBM furnizează corecții interimare și corecții de securitate pentru toate edițiile HMC suportate.

Cum sunt urmărite noile corecții interimare pentru HMC?

Buletinul de securitate conține informații despre vulnerabilitățile și corecțiile interimare pentru versiunile HMC suportate. Pentru a urmări corecțiile interimare pentru HMC, puteți să:

- Căutați cele mai recente buletine de securitate, la [IBM Security Bulletin](#).
- Urmăriți pe Twitter [@IBMPowereSupp](#) pentru notificări.
- Vă abonați la notificări prin e-mail, la [IBM Support](#).

Locațiile porturilor HMC

Puteți găsi locațiile porturilor utilizând codurile de locație. Folosiți ilustrațiile cu locațiile porturilor HMC pentru a asocia un cod de locație cu poziția portului HMC pe server.

Locațiile porturilor HMC pe modelul 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H și 9223-22S

Utilizați această diagramă și tabelă pentru a mapa porturile HMC pe 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H și 9223-22S.

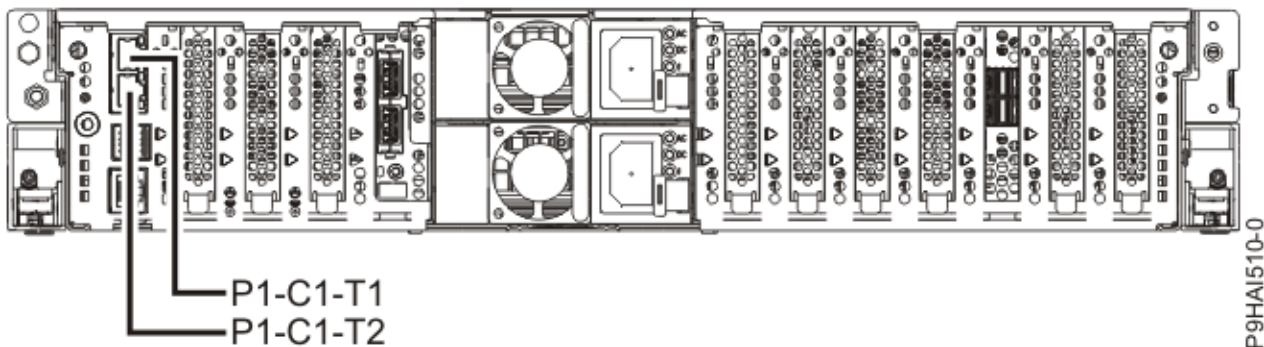


Figura 10. Locațiile porturilor HMC pe 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H și 9223-22S

Tabela 39. Locațiile porturilor HMC pe 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H și 9223-22S		
Port	Cod locație fizică	Led de identificare
Port HMC 1	Un-P1-C1-T1	Nu
Port HMC 2	Un-P1-C1-T2	Nu
Pentru informații suplimentare despre locațiile porturilor HMC pe 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H sau 9223-22S, vedeți Locațiile părților componente și codurile de locație pentru 9008-22L, 9009-22A, 9009-22G, 9223-22H sau 9223-22S .		

Locațiile porturilor HMC pe modelul 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H și 9223-42S

Utilizați această diagramă și tabelă pentru a mapa porturile HMC pe 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H și 9223-42S.

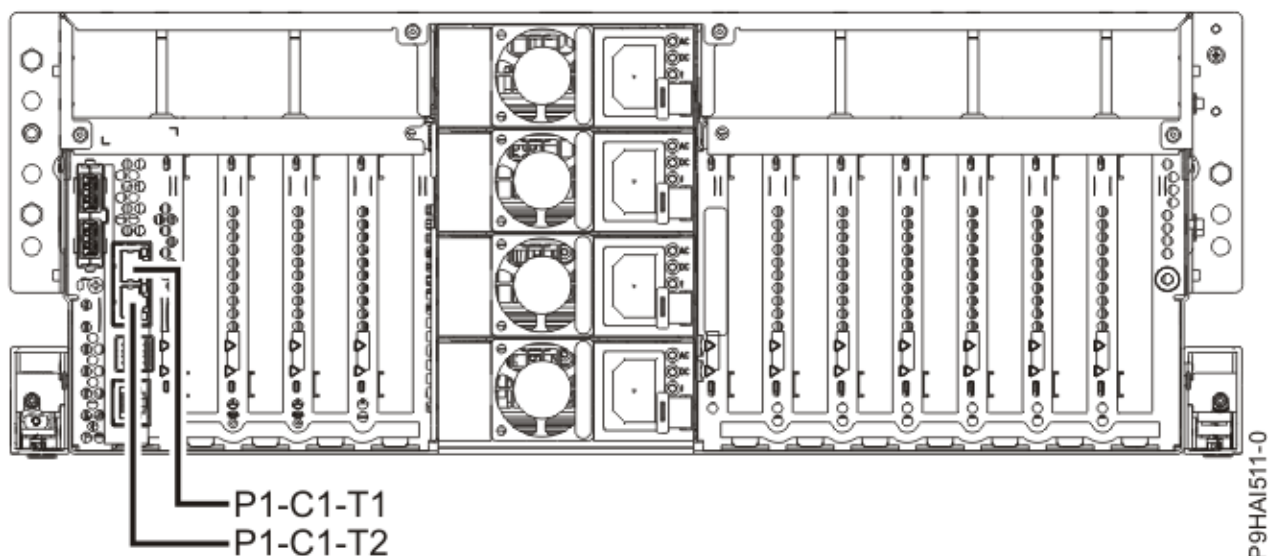


Figura 11. Locațiile porturilor HMC pe 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H și 9223-42S

Tabela 40. Locațiile porturilor HMC pe 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H și 9223-42S

Port	Cod locație fizică	Led de identificare
Port HMC 1	Un-P1-C1-T1	Nu
Port HMC 2	Un-P1-C1-T2	Nu

Pentru informații suplimentare despre locațiile porturilor HMC pe 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H sau 9223-42S, vedeți [Locațiile părților componente și codurile de locație pentru 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H sau 9223-42S](#).

Locațiile porturilor HMC pe modelul 9040-MR9

Folosiți această diagramă și acest tabel pentru a localiza porturile HMC pe 9040-MR9.

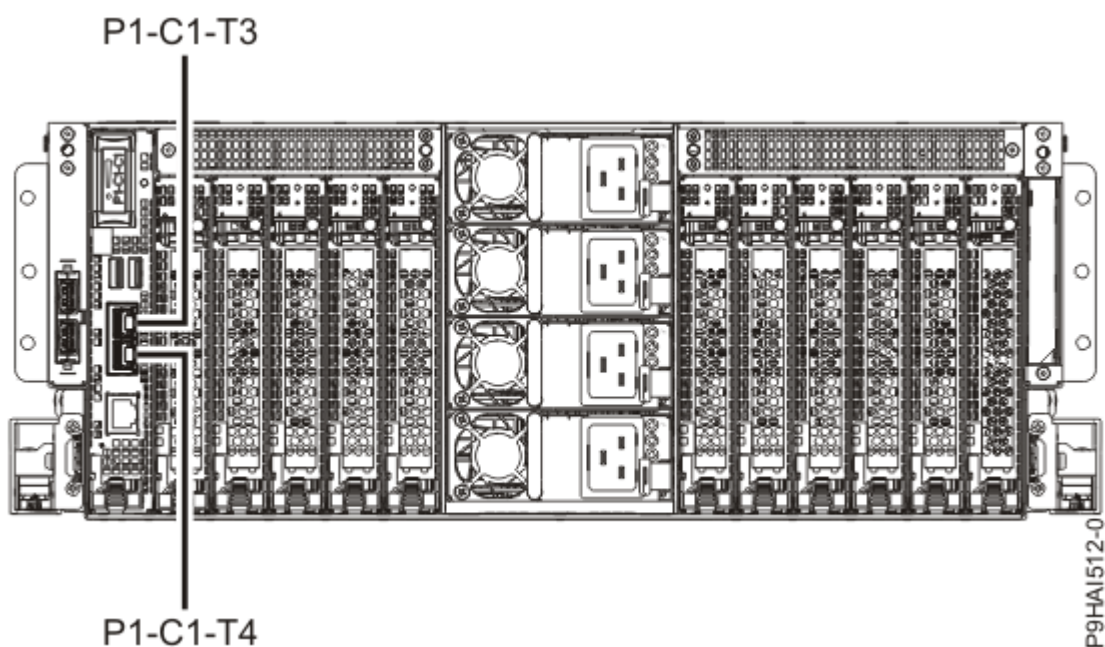


Figura 12. Locațiile porturilor HMC pe 9040-MR9

Tabela 41. Locațiile porturilor HMC pe 9040-MR9		
Port	Cod locație fizică	Led de identificare
Port HMC 1	Un-P1-C1-T3	Nu
Port HMC 2	Un-P1-C1-T4	Nu
Pentru informații suplimentare despre locațiile porturilor HMC pe 9040-MR9, vedeți Locațiile părților componente și codurile de locație .		

Locațiile porturilor HMC pe modelul 9080-M9S

Folosiți această diagramă și acest tabel pentru a localiza porturile HMC pe 9080-M9S.

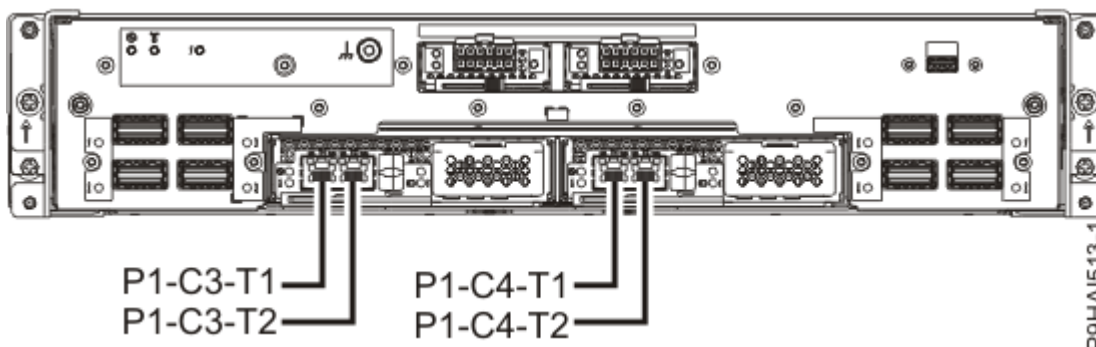


Figura 13. Locațiile porturilor HMC pe 9080-M9S

Tabela 42. Locațiile porturilor HMC pe 9080-M9S		
Port	Locație port fizic	Led de identificare
Placă procesor de service 1 - port HMC 1	Un-P1-C3-T1	Nu
Placă procesor de service 1 - port HMC 2	Un-P1-C3-T2	Nu
Placă procesor de service 2 - port HMC 1	Un-P1-C4-T1	Nu
Placă procesor de service 2 - port HMC 2	Un-P1-C4-T2	Nu
Pentru informații suplimentare despre locațiile porturilor HMC pe 9080-M9S, vedeți Locațiile părților componente și codurile de locație .		

Observații

Aceste informații au fost elaborate pentru produse și servicii oferite în Statele Unite.

Este posibil ca IBM să nu ofere în alte țări produsele, serviciile sau caracteristicile discutate în acest document. Consultați reprezentantul IBM local pentru informații despre produsele și serviciile disponibile curent în zona dumneavoastră. Referirea la un produs, program sau serviciu IBM product nu înseamnă că se afirmă sau se sugerează că poate fi utilizat numai produsul, programul sau serviciul IBM respectiv. Poate fi utilizat în locul acestuia orice produs, program sau serviciu echivalent funcțional care nu încalcă vreun drept de proprietate intelectuală al IBM. Însă este responsabilitatea utilizatorului să evalueze și să verifice operația oricărui produs, program sau serviciu non-IBM.

IBM poate avea brevete sau aplicații în curs de brevetare care să acopere subiectele descrise în acest document. Faptul că vi se furnizează acest document nu înseamnă că vi se acordă licența pentru aceste brevete. Puteți trimite întrebări cu privire la licențe, în scris, la:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

INTERNATIONAL BUSINESS MACHINES CORPORATION FURNIZEAZĂ ACEASTĂ PUBLICAȚIE "CA ATARE", FĂRĂ NICIUN FEL DE GARANȚIE, EXPLICITĂ SAU IMPLICITĂ, INCLUZÂND, DAR FĂRĂ A SE LIMITA LA, GARANȚIILE IMPLICITE DE NEÎNCĂLCARE A UNUI DREPT, DE VANDABILITATE SAU DE POTRIVIRE PENTRU UN ANUMIT SCOP. Unele jurisdicții nu permit declinarea responsabilității pentru garanțiile exprese sau implicite în anumite tranzacții și, de aceea, este posibil ca acest enunț să nu fie valabil în cazul dumneavoastră.

Aceste informații pot include inexactități tehnice sau erori tipografice. Informațiile incluse aici sunt modificate periodic; aceste modificări vor fi încorporate în noi ediții ale publicației. Este posibil ca IBM să aducă îmbunătățiri și/sau schimbări în produsele și/sau programele prezentate în această publicație, oricând și fără notificare.

Referirile din această publicație la site-uri Web non-IBM sunt oferite numai pentru a vă ajuta, fără ca prezența lor să însemne o susținere acordată acestor site-uri Web. Materialele de pe site-urile Web respective nu fac parte din materialele pentru acest produs IBM, iar utilizarea acestor site-uri Web se face pe propriul risc.

IBM poate utiliza sau distribui oricare dintre informațiile pe care le furnizați, în orice mod considerat adecvat, fără ca aceasta să implice vreo obligație pentru dumneavoastră.

Datele de performanță și exemplele referitoare la clienți sunt prezentate numai în scop ilustrativ. Rezultatele reale privind performanța pot varia în funcție de configurațiile și condițiile de operare specifice.

Informațiile referitoare la produsele non-IBM au fost obținute de la furnizorii produselor respective, din anunțurile lor publicate sau din alte surse disponibile public. IBM nu a testat aceste produse și nu poate confirma nivelul performanței, compatibilitatea sau alte calități pretinse ale acestor produse non-IBM. Întrebările despre capabilitățile produselor non-IBM trebuie să fie adresate furnizorilor acelor produse.

Declarațiile privind acțiunile viitoare sau intenția IBM pot fi schimbate sau retrase fără notificare, reprezentând doar posibile obiective.

Toate prețurile IBM sunt prețuri cu amănuntul sugerate de IBM, sunt actuale și pot fi modificate fără notificare. Prețurile dealer-ului pot varia.

Aceste informații sunt doar în scop de planificare. Informațiile menționate aici se pot modifica înainte ca produsele descrise să devină disponibile pe piață.

Aceste informații conțin exemple de date și rapoarte folosite în operațiile comerciale de zi cu zi. Pentru a le ilustra cât mai complet posibil, exemplele includ nume de persoane, companii, mărci și produse. Toate aceste nume sunt fictive și orice asemănare cu persoane sau companii reale este o pură coincidență.

Dacă vizualizați aceste informații în format electronic, este posibil să nu apară fotografiile și ilustrațiile color.

Desenele și specificațiile conținute aici nu vor fi reproduse, integral sau parțial, fără permisiunea scrisă a IBM.

IBM a pregătit aceste informații pentru folosirea cu mașinile specifice indicate. IBM nu sugerează în niciun fel că acestea pot fi utilizate pentru alte scopuri.

Sisteme de calcul ale IBM conțin mecanisme concepute pentru a reduce posibilitatea coruperii sau pierderii nedetectate a datelor. Însă acest risc nu poate fi eliminat. Utilizatorii care se confruntă cu opriri neplanificate, căderi ale sistemului, fluctuații sau întreruperi de tensiune sau defectarea unei componente trebuie să verifice acuratețea operațiilor efectuate și a datelor salvate sau transmise de către sistem la momentul întreruperii sau defecțiunii sau la un moment apropiat. În plus, utilizatorii trebuie să stabilească proceduri care să asigure o verificare independentă a datelor, pentru ca ele să poată fi considerate sigure în operațiile critice și sensibile. Utilizatorii trebuie să verifice periodic site-urile web de suport ale IBM, pentru informații de actualizare și corecții aplicabile sistemului și software-ului înrudit.

Declarație de omologare

Este posibil ca acest produs să nu fie certificat în țara dumneavoastră pentru conectarea prin orice mijloace la interfețele rețelelor publice de telecomunicații. Pentru a realiza o astfel de conexiune, legislația poate impune o certificare suplimentară. Contactați un reprezentant sau reseller IBM pentru întrebări.

Caracteristicile de accesibilitate pentru serverele IBM Power Systems

Caracteristicile de accesibilitate ajută utilizatorii cu dezabilități fizice, cum ar fi mobilitatea redusă sau vederea limitată, să utilizeze cu succes conținutul IT.

Privire generală

Serverele IBM Power Systems includ următoarele caracteristici majore de accesibilitate:

- Operarea numai cu tastatura
- Operațiile care utilizează un cititor de ecran

Serverele IBM Power Systems cel mai recent standard W3C, [WAI-ARIA 1.0](http://www.w3.org/TR/wai-aria/) (www.w3.org/TR/wai-aria/), pentru a asigura conformitatea cu [US Section 508](http://www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) (www.access-board.gov/guidelines-and-standards/communications-and-it/about-the-section-508-standards/section-508-standards) și [Web Content Accessibility Guidelines \(WCAG\) 2.0](http://www.w3.org/TR/WCAG20/) (www.w3.org/TR/WCAG20/). Pentru a beneficia de caracteristicile de accesibilitate, utilizați cea mai recentă versiune de cititor de ecran și cel mai recent browser web acceptat de serverele IBM Power Systems.

Documentația de produs online din IBM Knowledge Center pentru serverele IBM Power Systems este activată pentru accesibilitate. Caracteristicile de accesibilitate din IBM Knowledge Center sunt descrise în secțiunea [Accesibilitatea din ajutorul pentru IBM Knowledge Center](http://www.ibm.com/support/knowledgecenter/doc/kc_help.html#accessibility) (www.ibm.com/support/knowledgecenter/doc/kc_help.html#accessibility).

Navigarea de la tastatură

Acest produs utilizează tastele de navigare standard.

Informații privind interfața

Interfețele de utilizator ale serverelor IBM Power Systems nu au conținut cu afișare intermitentă de 2-55 ori pe secundă.

Interfețele de utilizator web ale serverelor IBM Power Systems se bazează pe foile de stil CSS (cascading style sheet) pentru a randa conținutul corespunzător și a furniza o experiență utilă. Aplicația furnizează o modalitate echivalentă pentru utilizatorii cu vedere redusă, pentru folosirea setărilor de sistem privind afișarea, inclusiv modul de contrast înalt. Puteți controla dimensiunea fontului utilizând setările dispozitivului sau ale browser-ului web.

Interfața de utilizator web a serverelor IBM Power Systems include repere de navigare WAI-ARIA, pe care le puteți utiliza pentru a naviga rapid către zonele funcționale din aplicație.

Software-ul de furnizor

Serverele IBM Power Systems includ anumite produse software de furnizor, care nu sunt acoperite de acordul de licență cu IBM. IBM nu face nicio declarație privind caracteristicile de accesibilitate ale acestor produse. Contactați furnizorul pentru informații privind accesibilitatea produselor sale.

Informații înrudite privind accesibilitatea

Pe lângă site-urile web IBM help desk și de suport, IBM are un serviciu telefonic TTY pentru utilizarea de către clienții surzi sau cu auz limitat, pentru accesarea serviciilor de vânzări și suport:

Serviciul TTY
800-IBM-3383 (800-426-3383)
(în America de Nord)

Pentru informații suplimentare despre angajamentul IBM privind accesibilitatea, consultați [IBM Accessibility \(www.ibm.com/able\)](http://www.ibm.com/able).

Considerente privind politica de confidențialitate

Produsele IBM Software, inclusiv soluțiile software ca serviciu, ("Ofertele Software") pot utiliza cookie-uri sau alte tehnologii pentru a colecta informații privind utilizarea produselor, pentru a ajuta la îmbunătățirea experienței utilizatorilor finali, ajustarea interacțiunilor la fiecare utilizator final sau pentru alte scopuri. În multe cazuri Ofertele Software nu colectează informații identificabile ca personale. Unele dintre Ofertele noastre Software vă pot ajuta să colectați informații identificabile ca personale. Dacă această Ofertă Software utilizează cookie-uri pentru a colecta informații identificabile ca personale, mai jos sunt prezentate informații specifice privind utilizarea cookie-urilor de către această ofertă.

În funcție de configurațiile livrate, această Ofertă software ar putea utiliza cookie-uri de sesiune care colectează pentru fiecare utilizator, numele de utilizator și adresa IP în scopuri de gestionare a sesiunilor. Aceste cookie-uri pot fi dezactivate, dar dezactivarea lor va elimina funcționalitatea pe care o activează acestea.

În cazul în care configurațiile livrate pentru această Ofertă Software vă furnizează abilitatea de a colecta informații identificabile ca personale de la utilizatorii finali, prin cookie-uri și alte tehnologii, ar trebui să solicitați consiliere juridică privind legislația aplicabilă pentru o astfel de colectare de date, inclusiv pentru cerințele privind notificarea și obținerea consimțământului.

Pentru informații suplimentare despre utilizarea diverselor tehnologii, inclusiv cookie-uri, pentru aceste scopuri, consultați Politica de confidențialitate IBM, la <http://www.ibm.com/privacy>, și IBM's Declarația privind confidențialitatea online, la <http://www.ibm.com/privacy/details/us/en/>, în secțiunea intitulată "Cookie-uri, beacon-uri Web și alte tehnologii".

Mărci comerciale

IBM, emblema IBM și [ibm.com](http://www.ibm.com) sunt mărci comerciale sau mărci comerciale înregistrate deținute de International Business Machines Corp., înregistrate în multe jurisdicții din întreaga lume. Alte nume de

produse sau de servicii pot fi mărci comerciale deținute de IBM sau de alte companii. Lista curentă cu mărcile comerciale IBM este disponibilă pe pagina web [Copyright and trademark information](#).

Marca înregistrată Linux este utilizată în baza unei sublicențe de la Linux Foundation, deținătorul exclusiv al licenței acordate de Linus Torvalds, proprietarul mărcii în întreaga lume.

Red Hat, JBoss, OpenShift, Fedora, Hibernate, Ansible, CloudForms, RHCA, RHCE, RHCSA, Ceph și Gluster sunt mărci comerciale sau mărci comerciale înregistrate deținute de Red Hat, Inc. sau de filialele sale în Statele Unite și în alte țări.

Microsoft și Windows sunt mărci comerciale ale Microsoft Corporation în Statele Unite, sau late țări sau ambele.

Java și toate emblemele și mărcile comerciale bazate pe Java sunt mărci comerciale sau mărci comerciale înregistrate deținute de Oracle și/sau afiliatele sale.

Observații privind emisia electronică

Observații privind Clasa A

Următoarele declarații privind Clasa A sunt valabile pentru serverele IBM care conțin procesorul POWER9 și caracteristicile sale, în afară de cazul în care sunt desemnate ca având Clasa B de compatibilitate electromagnetică (EMC) în informațiile de caracteristici.

Atunci când atașați un monitor la echipament, trebuie să utilizați cablul de monitor indicat și dispozitivele livrate cu monitorul pentru suprimarea interferenței.

Observație pentru Canada

CAN ICES-3 (A)/NMB-3(A)

Observație pentru Comunitatea Europeană și Maroc

Acest produs este în conformitate cu cerințele de protecție stipulate de Directiva 2014/30/EU a Parlamentului European și a Consiliului European privind armonizarea legilor statelor membre referitoare la compatibilitatea din punct de vedere electromagnetic. IBM nu poate accepta responsabilitatea pentru nerespectarea normelor de protecție ca urmare a unei modificări nerecomandate a produsului, inclusiv adaptarea unor plăci opționale non-IBM.

Acest produs ar putea provoca interferențe dacă este utilizat în zone rezidențiale. Ar trebui să fie evitată o astfel de utilizare, cu excepția cazurilor în care utilizatorul ia măsuri speciale pentru a reduce emisiile electromagnetice, astfel încât să nu se producă interferențe cu semnalele posturilor de radio și televiziune.

Avertisment: Acest echipament este în conformitate cu Clasa A din standardul CISPR 32. Într-un mediu rezidențial, acest echipament poate cauza interferențe radio.

Observație pentru Germania

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2014/30/EU zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 / EN 55032 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung von IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung von IBM gesteckt/eingebaut werden.

EN 55032 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden:

"Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen."

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem "Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)". Dies ist die Umsetzung der EU-Richtlinie 2014/30/EU in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC Richtlinie 2014/30/EU) für Geräte der Klasse A

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:

International Business Machines Corp.

New Orchard Road

Armonk, New York 10504

Tel: 914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:

IBM Deutschland GmbH

Technical Relations Europe, Abteilung M456

IBM-Allee 1, 71139 Ehningen, Germany

Tel: +49 (0) 800 225 5426

e-mail: HalloIBM@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 / EN 55032 Klasse A.

Observație pentru JEITA (Japan Electronics and Information Technology Industries Association)

(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

Această declarație este valabilă pentru produsele cu 20 A sau mai puțin per fază.

高調波電流規格 JIS C 61000-3-2 適合品

Această declarație este valabilă pentru produsele monofazate cu mai mult de 20 A.

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

Această declarație este valabilă pentru produsele trifazate cu mai mult de 20 A.

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

Observație pentru VCCI (Voluntary Control Council for Interference) în Japonia

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

Observație pentru Coreea

이 기기는 업무용 환경에서 사용할 목적으로 적합성평가를 받은 기기로서 가정용 환경에서 사용하는 경우 전파간섭의 우려가 있습니다.

Observație pentru Republica Populară Chineză

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。

Observație pentru Rusia

ВНИМАНИЕ! Настоящее изделие относится к классу А. В жилых помещениях оно может создавать радиопомехи, для снижения которых необходимы дополнительные меры

Observație pentru Taiwan

警告使用者：

此為甲類資訊技術設備，
於居住環境中使用時，可
能會造成射頻擾動，在此
種情況下，使用者會被要
求採取某些適當的對策。

Informații de contact IBM Taiwan:

台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

Observație FCC (Federal Communications Commission) pentru Statele Unite

Acest echipament a fost testat și s-a constatat că respectă limitele pentru un dispozitiv digital din Clasa A, conform cerințelor stipulate de Partea a 15-a din Regulile FCC. Aceste limite au fost impuse pentru a asigura o protecție rezonabilă împotriva interferențelor dăunătoare când echipamentul este operat într-un mediu comercial. Acest echipament generează, utilizează și poate radia energie de radiofrecvență, iar atunci când nu este instalat și utilizat conform instrucțiunilor poate produce interferențe care să afecteze comunicațiile radio. Operarea acestui echipament într-o zonă rezidențială poate cauza interferențe nocive, caz în care utilizatorul trebuie să corecteze aceste interferențe pe cheltuiala proprie.

Pentru a respecta limitele FCC privind emisia, trebuie să fie utilizate cabluri și conectori cu ecranare și legare la pământ corespunzătoare. Aceste condiții sunt îndeplinite de cablurile și conectorii pe care îi furnizează dealer-ii autorizați de IBM. IBM nu își asumă responsabilitatea pentru niciun fel de interferențe, radio sau TV, cauzate de utilizarea altor cabluri sau conectori decât versiunile recomandate sau modificări neautorizate ale acestui echipament. Modificările neautorizate pot anula autorizarea utilizatorului de a opera echipamentul.

Acest dispozitiv este

în conformitate cu Partea a 15-a din regulile FCC. Operarea se face cu respectarea următoarelor două condiții:

(1) nu este permis ca acest dispozitiv să genereze interferențe dăunătoare și (2) acest dispozitiv trebuie să accepte orice interferență receptată, inclusiv interferențele ce pot determina o funcționare improprie.

Partea responsabilă:

International Business Machines Corporation

New Orchard Road

Armonk, NY 10504

Contact numai pentru informații privind conformitatea cu FCC: fccinfo@us.ibm.com

Observații privind Clasa B

Următoarele declarații privind Clasa B sunt valabile pentru caracteristicile desemnate în informațiile de instalare a caracteristicii ca fiind din Clasa B de compatibilitate electromagnetică.

Atunci când atașați un monitor la echipament, trebuie să utilizați cablul de monitor indicat și dispozitivele livrate cu monitorul pentru suprimarea interferenței.

Observație pentru Canada

CAN ICES-3 (B)/NMB-3(B)

Observație pentru Comunitatea Europeană și Maroc

Acest produs este în conformitate cu cerințele de protecție stipulate de Directiva 2014/30/EU a Parlamentului European și a Consiliului European privind armonizarea legilor statelor membre referitoare la compatibilitatea din punct de vedere electromagnetic. IBM nu poate accepta responsabilitatea pentru nerespectarea normelor de protecție ca urmare a unei modificări nerecomandate a produsului, inclusiv adaptarea unor plăci opționale non-IBM.

Observație în germană

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse B EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2014/30/EU zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022/ EN 55032 Klasse B ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung von IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung von IBM gesteckt/eingebaut werden.

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem "Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)". Dies ist die Umsetzung der EU-Richtlinie 2014/30/EU in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC Richtlinie 2014/30/EU) für Geräte der Klasse B

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:
International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
Tel: 914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:
IBM Deutschland GmbH
Technical Relations Europe, Abteilung M456
IBM-Allee 1, 71139 Ehningen, Germany
Tel: +49 (0) 800 225 5426
e-mail: HalloIBM@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55032 Klasse B

Observație pentru JEITA (Japan Electronics and Information Technology Industries Association)

(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

Această declarație este valabilă pentru produsele cu 20 A sau mai puțin per fază.

高調波電流規格 JIS C 61000-3-2 適合品

Această declarație este valabilă pentru produsele monofazate cu mai mult de 20 A.

高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。

- 回路分類 : 6 (単相、P F C回路付)
- 換算係数 : 0

Această declarație este valabilă pentru produsele trifazate cu mai mult de 20 A.

高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。

- 回路分類 : 5 (3相、P F C回路付)
- 換算係数 : 0

Observație pentru VCCI (Voluntary Control Council for Interference) în Japonia

この装置は、クラスB情報技術装置です。この装置は、家庭環境で使用するを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをして下さい。

VCCI-B

Observație pentru Taiwan

台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

Observație FCC (Federal Communications Commission) pentru Statele Unite

Acest echipament a fost testat și s-a constatat că respectă limitele pentru un dispozitiv digital din Clasa B, conform cerințelor stipulate de Partea a 15-a din Regulile FCC. Aceste limite au fost impuse pentru a asigura o protecție rezonabilă împotriva interferențelor dăunătoare în cazul instalării într-o locuință. Acest echipament generează, utilizează și poate radia energie de radiofrecvență, iar atunci când nu este instalat și utilizat conform instrucțiunilor poate produce interferențe care să afecteze comunicațiile radio. Însă nu se poate garanta că nu vor apărea interferențe într-o anumită instalare. Dacă acest echipament cauzează o interferență ce afectează recepția emisiunilor de radio sau televiziune, lucru ce poate fi constatat oprind și pornind echipamentul, se recomandă utilizatorului să încerce diminuarea interferenței aplicând una dintre următoarele măsuri:

- Reorientarea sau re poziționarea antenei de recepție.
- Mărirea distanței dintre echipament și receptor.
- Conectarea echipamentului la o priză aflată pe un circuit diferit de cel al receptorului.
- Consultarea unui dealer autorizat de IBM sau a unei reprezentant de service pentru ajutor.

Pentru a respecta limitele FCC privind emisia, trebuie să fie utilizate cabluri și conectori cu ecranare și legare la pământ corespunzătoare. Aceste condiții sunt îndeplinite de cablurile și conectorii pe care îi furnizează dealer-ii autorizați de IBM. IBM nu își asumă responsabilitatea pentru niciun fel de interferențe, radio sau TV, cauzate de utilizarea altor cabluri sau conectori decât versiunile recomandate sau modificări neautorizate ale acestui echipament. Modificările neautorizate pot anula autorizarea utilizatorului de a opera echipamentul.

Acest dispozitiv este în conformitate cu Partea a 15-a din regulile FCC. Operarea se face cu respectarea următoarelor două condiții:

(1) nu este permis ca acest dispozitiv să genereze interferențe dăunătoare și (2) acest dispozitiv trebuie să accepte orice interferență receptată, inclusiv interferențele ce pot determina o funcționare improprie.

Partea responsabilă:

International Business Machines Corporation
New Orchard Road
Armonk, New York 10504

Contact numai pentru informații privind conformitatea cu FCC: fccinfo@us.ibm.com

Termeni și condiții

Permisunile pentru folosirea acestor publicații sunt acordate în baza termenilor și condițiilor următoare.

Aplicabilitate: Acești termeni și aceste condiții vin în completarea oricăror termeni de utilizare pentru site-ul web IBM.

Utilizare personală: Puteți reproduce aceste publicații pentru utilizarea personală, necomercială, cu condiția ca toate anunțurile de proprietate să fie păstrate. Nu puteți să distribuiți, să afișați sau să realizați lucrări derivate din aceste publicații sau dintr-o porțiune a lor fără consimțământul explicit al IBM.

Utilizare comercială: Puteți reproduce, distribui și afișa aceste publicații doar în cadrul întreprinderii dumneavoastră, cu condiția ca toate anunțurile de proprietate să fie păstrate. Nu puteți să realizați lucrări derivate din aceste informații, nici să reproduceți, să distribuiți sau să afișați aceste informații sau o porțiune a lor în afara întreprinderii dumneavoastră fără consimțământul explicit al IBM.

Drepturi: Cu excepția celor acordate explicit prin această permisiune, nu mai sunt acordate alte permisiuni, licențe sau drepturi, explicite sau implicite, pentru publicații sau pentru orice informație, date, software sau alte proprietăți intelectuale pe care le conțin acestea.

IBM își rezervă dreptul de a retrage permisiunile acordate aici oricând consideră că utilizarea publicațiilor contravine interesului său sau când IBM stabilește că instrucțiunile de mai sus nu sunt urmate corespunzător.

Nu puteți descărca, exporta sau reexporta aceste informații decât cu condiția respectării integrale a legilor și regulamentelor în vigoare, precum și a legilor și regulamentelor din Statele Unite privind exportul.

IBM NU GARANTEAZĂ CONȚINUTUL ACESTOR PUBLICAȚII. PUBLICAȚIILE SUNT FURNIZATE "CA ATARE", FĂRĂ NICIUN FEL DE GARANȚIE, EXPLICITĂ SAU IMPLICITĂ, INCLUZÂND, DAR FĂRĂ A SE LIMITA LA, GARANȚIILE IMPLICITE DE VANDABILITATE, DE NEÎNCĂLCARE A UNUI DREPT SAU DE POTRIVIRE PENTRU UN ANUMIT SCOP.

