

Power Systems

*Instalowanie i konfigurowanie konsoli
HMC*



Uwaga

Przed wykorzystaniem tych informacji i użyciem produktu, którego dotyczą, należy zapoznać się z sekcjami “Uwagi dotyczące bezpieczeństwa” na stronie v i “Uwagi” na stronie 105 oraz podręcznikami *IBM Systems Safety Notices* (G229-9054) i *IBM Environmental Notices and User Guide* (Z125-5823).

Niniejsze wydanie dotyczy konsoli IBM® Hardware Management Console, wersja 9, wydanie 2, poziom poprawek 950, oraz wszystkich późniejszych wersji i modyfikacji, chyba że w nowych wydaniach zostanie określone inaczej.

© Copyright International Business Machines Corporation 2018, 2021.

Spis treści

Uwagi dotyczące bezpieczeństwa.....	v
Instalowanie i konfigurowanie konsoli HMC.....	1
Co nowego w sekcji Instalowanie i konfigurowanie konsoli HMC.....	1
Zadania instalowania i konfigurowania.....	2
Instalowanie i konfigurowanie nowej konsoli HMC z nowym serwerem.....	2
Aktualizowanie kodu konsoli HMC.....	3
Dodawanie drugiej konsoli HMC do istniejącej instalacji.....	3
Instalowanie konsoli HMC.....	4
Instalowanie serwera IBM Power Systems HMC (7063-CR2) w stelażu.....	4
Instalowanie systemu 7063-CR1 w stelażu.....	14
Instalowanie wirtualnego urządzenia konsoli HMC	25
Konfigurowanie konsoli HMC.....	40
Wybór ustawień sieciowych konsoli HMC.....	40
Konfigurowanie konsoli HMC.....	57
Czynności pokonfiguracyjne.....	79
Aktualizowanie i migrowanie kodu maszynowego konsoli HMC.....	80
Zabezpieczanie konsoli HMC.....	92
Rozszerzona strategia hasel.....	94
Profil zabezpieczeń: RODO i PCI-DSS (Payment Card Industry Data Security Standard)	96
Rozwiązywanie najczęstszych problemów podczas zabezpieczania konsoli HMC.....	97
Położenie portów konsoli HMC.....	100
Uwagi.....	105
Ułatwienia dostępu dla serwerów IBM Power Systems.....	106
Postanowienia dotyczące ochrony prywatności	107
Znaki towarowe.....	108
Uwagi dotyczące emisji promieniowania elektromagnetycznego.....	108
Uwagi dotyczące produktów klasy A.....	108
Uwagi dotyczące produktów klasy B.....	111
Warunki.....	114

Uwagi dotyczące bezpieczeństwa

Uwagi dotyczące bezpieczeństwa, które mogą być zamieszczone w różnych miejscach niniejszego podręcznika:

- Uwaga dotycząca **NIEBEZPIECZEŃSTWA** zawiera omówienie sytuacji, która stanowi potencjalne zagrożenie zdrowia lub życia.
- Uwaga dotycząca **ZAGROŻENIA** zawiera omówienie sytuacji, która w pewnych warunkach może stanowić zagrożenie.
- Uwaga dotycząca **OSTRZEŻENIA** zawiera omówienie sytuacji, która może spowodować uszkodzenie programu, urządzenia, systemu lub danych.

Informacje dotyczące bezpieczeństwa w handlu ogólnosiwiatowym

Niektóre kraje wymagają tłumaczenia informacji dotyczących bezpieczeństwa zawartych w publikacjach dotyczących produktu na języki narodowe. Jeśli wymaganie to ma zastosowanie do kraju użytkownika, wówczas dokumentacja z informacjami dotyczącymi bezpieczeństwa dołączona jest do pakietu publikacji (w wersji drukowanej, na dysku DVD lub jako element produktu) dostarczanego wraz z produktem. Dokumentacja zawiera informacje dotyczące bezpieczeństwa w języku narodowym oraz odniesienie do informacji źródłowych w języku angielskim. Przed przystąpieniem do korzystania z publikacji w języku angielskim w związku z instalowaniem, uruchamianiem lub serwisowaniem produktu, należy najpierw zapoznać się z informacjami dotyczącymi jego bezpieczeństwa, zawartymi w dokumentacji. Należy również sprawdzać informacje w dokumentacji w przypadku niezrozumienia jakichkolwiek informacji dotyczących bezpieczeństwa w publikacjach w języku angielskim.

Aby otrzymać kopię zastępczą lub dodatkowe kopie informacji dotyczących bezpieczeństwa, należy skontaktować się z IBM pod numerem telefonu 1-800-300-8751.

German safety information

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

Informacje dotyczące bezpieczeństwa użytkowania produktów laserowych

Serwery IBM mogą wykorzystywać karty lub opcje we/wy oparte na technologii światłowodowej i wykorzystujące lasery lub diody LED.

Zgodność produktów laserowych

Serwery IBM mogą być zainstalowane zarówno wewnątrz, jak i na zewnątrz stelaża na urządzenia informatyczne.



NIEBEZPIECZEŃSTWO: Podczas pracy z systemem lub w jego pobliżu należy przestrzegać następujących środków ostrożności:

Napięcie i prąd elektryczny, przepływający przez kable zasilające, telefoniczne i komunikacyjne, stanowią zagrożenie. Aby uniknąć niebezpieczeństwa porażenia prądem elektrycznym: jeśli zostały dostarczone kable zasilające IBM, to zasilanie tej jednostki można podłączać jedynie za pomocą takich dostarczonych kabli IBM. Nie należy używać dostarczonego kabla zasilającego IBM z jakimkolwiek innym produktem. Nie należy otwierać ani serwisować żadnego zespołu zasilacza. Nie należy podłączać ani odłączać żadnych kabli, ani też przeprowadzać instalacji, konserwacji czy ponownej konfiguracji tego produktu podczas burzy z wyładowaniami atmosferycznymi.



- Produkt może być wyposażony w wiele kabli zasilających. Aby wyeliminować niebezpieczne napięcie, należy odłączyć je wszystkie. W przypadku zasilania prądem przemiennym należy odłączyć wszystkie kable zasilające od źródła zasilania. W przypadku stelaży wyposażonych w tablicę rozdzielczą zasilania prądem stałym (PDP) należy odłączyć źródło zasilania prądem stałym od tablicy PDP.
- Podczas podłączania zasilania należy upewnić się, że wszystkie kable zasilające są poprawnie podłączone. W przypadku stelaży zasilanych prądem przemiennym należy podłączyć wszystkie kable zasilające do prawidłowo okablowanego i uziemionego gniazda elektrycznego. Należy upewnić się, że gniazdo zasilające zapewnia właściwe napięcie i kolejność faz, zgodnie z tabliczką znamionową systemu. W przypadku stelaży wyposażonych w tablicę rozdzielczą zasilania prądem stałym (PDP) należy podłączyć źródło zasilania prądem stałym do tablicy PDP. Podczas podłączania kabli zasilających prądem stałym (doprowadzających i powrotnych) należy się upewnić, że polaryzacja jest poprawna.
- Należy podłączyć wszystkie podłączone do tego produktu urządzenia do prawidłowo okablowanych gniazd zasilających.
- Jeśli to możliwe, należy podłączać i odłączać kable sygnałowe jedną ręką.
- Nigdy nie należy włączać urządzeń, jeśli widoczne są ślady świadczące o działaniu ognia, wody lub istnieniu uszkodzeń konstrukcji.
- Nie należy podejmować prób włączenia zasilania maszyny do czasu wyeliminowania wszelkich sytuacji mogących spowodować zagrożenie.
- Podczas sprawdzania urządzenia należy zawsze zakładać, że występuje zagrożenie dla bezpieczeństwa ze strony prądu elektrycznego. Podczas instalowania podsystemu należy wykonać wszystkie kontrole ciągłości, uziemienia i zasilania w celu zagwarantowania spełniania przez maszynę wymogów dotyczących bezpieczeństwa. Nie należy podejmować prób włączenia zasilania maszyny do czasu wyeliminowania wszelkich sytuacji mogących spowodować zagrożenie. Jeśli procedury instalacji i konfiguracji nie stanowią inaczej, to przed otwarciem obudowy urządzenia należy odłączyć kable zasilające prądem przemiennym, wyłączyć odpowiednie wyłączniki automatyczne na tablicy rozdzielczej zasilania (PDP) oraz odłączyć kable systemów telekomunikacyjnych, sieci i modemów.
- Podczas instalacji i przemieszczania tego produktu lub podłączonych do niego urządzeń, a także podczas otwierania ich obudów, kable należy podłączać i odłączać według poniższego opisu.

Aby odłączyć: 1) wyłącz wszystko (o ile instrukcja nie zawiera innej informacji). 2) W przypadku zasilania prądem przemiennym wyjmij wszystkie kable zasilające z gniazd. 3) W przypadku stelaży wyposażonych w tablicę rozdzielczą zasilania prądem stałym (PDP) wyłącz wyłączniki automatyczne na tablicy PDP i odłącz zasilanie od źródła prądu stałego u klienta. 4) Odłącz kable sygnałowe od złączy. 5) Odłącz wszystkie kable od urządzeń.

Aby podłączyć: 1) wyłącz wszystko (o ile instrukcja nie zawiera innej informacji). 2) Podłącz wszystkie kable do urządzeń. 3) Podłącz kable sygnałowe do złączy. 4) W przypadku zasilania prądem przemiennym podłącz wszystkie kable zasilające do gniazd. 5) W przypadku stelaży wyposażonych w tablicę rozdzielczą zasilania prądem stałym (PDP) przywróć zasilanie ze źródła zasilania prądem stałym u klienta i włącz wyłącznik automatyczny na tablicy PDP. 6) Włącz urządzenia.



- System może mieć ostre krawędzie, narożniki i złącza. Przy obsłudze urządzenia należy zachować ostrożność, aby uniknąć przecięć, zadrapań i przytrzaśnieć. (D005)

(R001 część 1 z 2):



NIEBEZPIECZEŃSTWO: Podczas pracy z systemem lub w jego pobliżu należy przestrzegać następujących środków ostrożności:

- Urządzenie jest ciężkie – niewłaściwa obsługa może spowodować obrażenia lub uszkodzenie urządzenia.
- Należy zawsze dokręcać nakrętki poziomujące stelaża.

- Należy zawsze instalować na stelażu klamry stabilizatora (jeśli zostały dostarczone), chyba że przewidziana jest instalacja opcji zabezpieczającej przed skutkami trzęsienia ziemi.
- Aby zapobiec niebezpieczeństwu związanemu z nierównomiernym obciążeniem, należy zawsze instalować najcięższe urządzenia w dolnej części stelaża. Instalowanie serwerów i urządzeń opcjonalnych należy zawsze rozpoczynać od dołu stelaża.
- Urządzenia stelażowe nie mogą spełniać funkcji półek ani powierzchni roboczych. Nie należy na nich umieszczać żadnych przedmiotów. Ponadto nie należy opierać się o urządzenia stelażowe ani używać ich do podtrzymywania równowagi (na przykład podczas pracy na drabinie).



- Niebezpieczeństwo utraty stabilności:
 - Stelaż może się przewrócić, powodując poważne obrażenia.
 - Przed wysunięciem stelaża do położenia instalacyjnego należy zapoznać się z instrukcjami dotyczącymi instalacji.
 - Nie należy w żaden sposób obciążać urządzeń zamontowanych w prowadnicach wysuwanych i znajdujących się w położeniu instalacyjnym.
 - Nie należy pozostawiać urządzeń zamontowanych w prowadnicach wysuwanych w położeniu instalacyjnym.
- Każdy stelaż może być wyposażony w kilka kabli zasilających.
 - W przypadku stelaży zasilanych prądem przemiennym należy odłączyć wszystkie kable zasilające stelaża, jeśli wymagane jest odłączenie zasilania.
 - W przypadku stelaży wyposażonych w tablicę rozdzielczą zasilania prądem stałym należy wyłączyć wyłącznik automatyczny doprowadzający zasilanie do jednostek systemowych lub odłączyć źródło zasilania prądem stałym u klienta, jeśli instrukcje nakazują odłączenie zasilania podczas serwisowania.
- Należy podłączyć wszystkie urządzenia zainstalowane w stelażu do urządzeń zasilających zainstalowanych w tym samym stelażu. Nie należy podłączać kabla zasilającego z urządzenia zainstalowanego w jednym stelażu do urządzenia zasilającego zainstalowanego w innym stelażu.
- Gniazdo elektryczne, które nie jest poprawnie okablowane, może spowodować wystąpienie niebezpiecznego napięcia na metalowych częściach systemu lub podłączanych do niego urządzeń. Odpowiedzialność za poprawne okablowanie i uziemienie gniazd zasilających w celu zabezpieczenia przed porażeniem prądem elektrycznym spoczywa na użytkowniku. (R001 część 1 z 2)

(R001 część 2 z 2):



UWAGA:

- Nie należy instalować jednostki w stelażu, jeśli temperatura otoczenia przekracza temperaturę otoczenia zalecaną przez producenta dla wszystkich urządzeń instalowanych w stelażu.
- Nie należy instalować jednostki w stelażu, w którym nie ma swobodnego przepływu powietrza. Należy zapewnić swobodny przepływ powietrza po bokach oraz z przedniej i tylnej strony jednostki na potrzeby wentylacji.
- Należy uważnie podłączyć sprzęt do obwodu zasilającego, tak aby przeciążenie obwodów nie uszkodziło okablowania zasilającego lub bezpieczników. Aby zapewnić prawidłowe podłączenie zasilania do stelaża, należy zapoznać się z etykietami znamionowymi znajdującymi się na urządzeniach w stelażu i obliczyć wymaganą łączną moc obwodu zasilającego.
- *(W przypadku szuflad wysuwanych).* Nie należy wysuwać ani instalować szuflad ani innych elementów, jeśli wsporniki stabilizatora stelaża przemysłowego nie są przymocowane do stelaża lub sam stelaż nie jest przykręcony do podłogi. Nie należy wysuwać dwu lub więcej szuflad jednocześnie. Po wysunięciu kilku szuflad jednocześnie stelaż może utracić stabilność.



- (W przypadku szuflad zamocowanych na stałe). Szuflada ta jest zamocowana na stałe i nie może być wyjmowana w celu dokonania czynności serwisowych, chyba że producent określi inaczej. Próba całkowitego lub częściowego wyjęcia szuflady ze stelaża może spowodować utratę stabilności stelaża lub wypadnięcie szuflady ze stelaża. (R001 część 2 z 2)



UWAGA: Usunięcie komponentów z górnych pozycji stelaża poprawia jego stabilność podczas przemieszczania. Podczas przemieszczania zapełnionego stelaża wewnątrz pomieszczenia lub budynku należy przestrzegać niniejszych ogólnych wytycznych:

- Należy zmniejszyć wagę stelaża przemysłowego, usuwając urządzenia poczynawszy od góry stelaża. Jeśli to możliwe, należy przywrócić konfigurację stelaża do takiej, w jakiej został on dostarczony. Jeśli jest ona nieznana, należy wykonać poniższe czynności:
 - Zdemontować wszystkie urządzenia zainstalowane na pozycji 32U i wyżej.
 - Sprawdzić, czy najcięższe urządzenia zostały zainstalowane na dole stelaża przemysłowego.
 - Upewnić się, że między urządzeniami zainstalowanymi poniżej pozycji 32U nie ma pustych pozycji U (lub jest ich niewiele), chyba że jest to jawnie dozwolone w otrzymanej konfiguracji.
- Jeśli przemieszczany stelaż przemysłowy stanowi część pakietu stelaży przemysłowych, należy odłączyć stelaż od pakietu.
- Jeśli przemieszczany stelaż został dostarczony z demontowalnymi wysięgnikami, należy je reinstalować przed przemieszczeniem stelaża.
- Należy sprawdzić planowaną trasę, aby wyeliminować potencjalne zagrożenia.
- Należy sprawdzić, czy wybrana trasa utrzyma ciężar załadowanego stelaża przemysłowego. Wagę załadowanego stelaża należy sprawdzić w dokumentacji dostarczonej wraz ze stelażem przemysłowym.
- Należy sprawdzić, czy wszystkie prześwity drzwi mają wymiary co najmniej 760 x 2083 mm (30 x 82 cale).
- Należy sprawdzić, czy wszystkie urządzenia, półki, szuflady, drzwi oraz kable zostały zabezpieczone.
- Należy sprawdzić, czy wszystkie cztery nakrętki poziomujące zostały podniesione do ich najwyższych pozycji.
- Należy sprawdzić, czy podczas przemieszczania w stelażu przemysłowym nie pozostały zainstalowane żadne klamry stabilizatora.
- Nie należy korzystać z rampy nachylonej pod kątem większym niż 10 stopni.
- Po przemieszczeniu stelaża należy:
 - Opuścić cztery nakrętki poziomujące.
 - Zainstalować klamry stabilizatora na stelażu przemysłowym lub – na obszarach zagrożonych trzęsieniami ziemi – przykręcić stelaż do podłogi.

- Jeśli ze stelaża zostały usunięte urządzenia, należy je ponownie zainstalować począwszy od najniższej pozycji do najwyższej.
- Jeśli wymagane jest przemieszczenie na dużą odległość, należy przywrócić pierwotną konfigurację stelaża. Należy zapakować stelaż w oryginalne opakowanie lub jego odpowiednik. Należy także opuścić nakrętki poziomujące, aby podnieść rolki ponad paletę i przymocować stelaż do palety.

(R002)

(L001)



NIEBEZPIECZEŃSTWO: Wewnątrz komponentu oznaczonego tą etykietą występuje napięcie lub natężenie prądu stanowiące zagrożenie dla zdrowia lub życia. Nie należy otwierać obudowy lub pokrywy z niniejszą etykietą. (L001)

(L002)

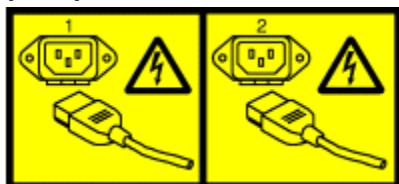


NIEBEZPIECZEŃSTWO: Urządzenia stelażowe nie mogą spełniać funkcji półek ani powierzchni roboczych. Nie należy na nich umieszczać żadnych przedmiotów. Ponadto nie należy opierać się o urządzenia stelażowe ani używać ich do podtrzymywania równowagi (na przykład podczas pracy na drabinie). Niebezpieczeństwo utraty stabilności:

- Stelaż może się przewrócić, powodując poważne obrażenia.
- Przed wysunięciem stelaża do położenia instalacyjnego należy zapoznać się z instrukcjami dotyczącymi instalacji.
- Nie należy w żaden sposób obciążać urządzeń zamontowanych w prowadnicach wysuwanych i znajdujących się w położeniu instalacyjnym.
- Nie należy pozostawiać urządzeń zamontowanych w prowadnicach wysuwanych w położeniu instalacyjnym.

(L002)

(L003)



lub



lub

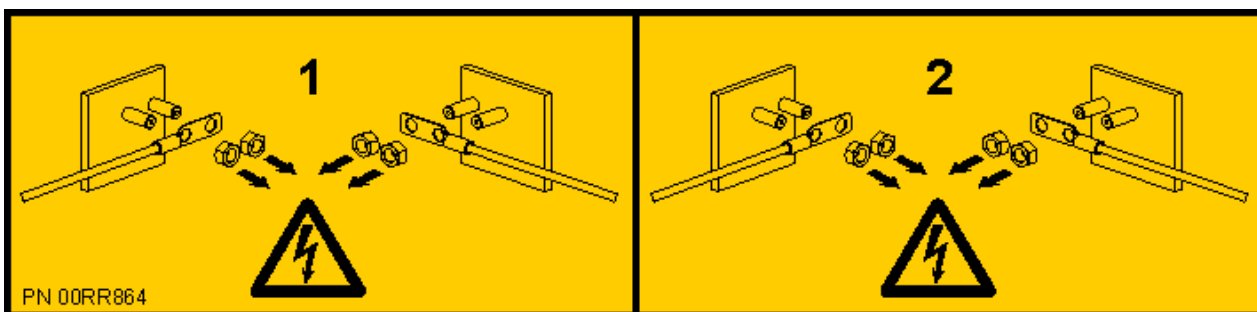


lub



lub





NIEBEZPIECZEŃSTWO: Wiele kabli zasilających. Produkt może być wyposażony w wiele kabli zasilających prądem przemiennym lub wiele kabli zasilających prądem stałym. Aby wyeliminować niebezpieczne napięcie, należy odłączyć wszystkie kable zasilające. (L003)

(L007)



UWAGA: Gorąca powierzchnia w pobliżu. (L007)

(L008)



UWAGA: Niebezpieczne ruchome części w pobliżu. (L008)

Wszystkie produkty laserowe posiadają w Stanach Zjednoczonych certyfikat zgodności z wymaganiami określonymi w dokumencie DHHS 21 CFR, Podrozdział J dla produktów laserowych klasy 1. Poza granicami Stanów Zjednoczonych produkty posiadają certyfikat zgodności z normą IEC 60825 jako produkty laserowe klasy 1. Informacje o numerach przyznanych certyfikatów i o organach zatwierdzających znajdują się na etykietach na poszczególnych częściach.



UWAGA: Produkt ten może zawierać co najmniej jedno z następujących urządzeń: napęd CD-ROM, napęd DVD-ROM, napęd DVD-RAM lub moduł lasera, będący produktem laserowym klasy 1. Należy zwrócić uwagę na następujące informacje:

- Nie należy zdejmować obudowy. Usunięcie obudowy produktu laserowego może spowodować kontakt z niebezpiecznym promieniowaniem lasera. Urządzenie nie zawiera części serwisowalnych.
- Użycie elementów sterujących, ustawień lub procedur innych niż opisane tutaj może spowodować zagrożenie niebezpiecznym promieniowaniem.

(C026)



UWAGA: W skład środowisk przetwarzania danych mogą wchodzić urządzenia przekazujące dane łączami systemowymi, zawierające moduły laserowe, które emitują promieniowanie powyżej klasy 1. Z tego powodu nie należy patrzeć na zakończenie kabla światłowodowego lub otwierać gniazda elektrycznego. Choć skierowanie jednego końca odłączonego światłowodu w stronę źródła światła i spojrzenie w drugi koniec w celu sprawdzenia ciągłości kabla nie musi spowodować

uszkodzenia oka, takie postępowanie jest potencjalnie niebezpieczne. Dlatego też nie zalecamy sprawdzania ciągłości światłowodu w ten sposób. Ciągłość kabla światłowodowego należy sprawdzać przy użyciu źródła światła i miernika mocy. (C027)



UWAGA: Ten produkt zawiera laser klasy 1M. Nie należy oglądać go bezpośrednio za pomocą instrumentów optycznych. (C028)



UWAGA: Niektóre produkty laserowe zawierają wbudowaną diodę laserową klasy 3A lub 3B. Należy zwrócić uwagę na następujące informacje:

- Jeśli produkt jest otwarty, występuje emisja promieniowania laserowego.
- Nie należy patrzeć na promień lasera ani oglądać go bezpośrednio za pomocą instrumentów optycznych. Należy unikać bezpośredniego kontaktu z promieniem. (C030)

(C030)



UWAGA: Akumulator zawiera lit. Aby uniknąć możliwości eksplozji, akumulatora nie można spalać ani ładować.

Akumulatora nie należy:

- wrzucać do wody ani go w niej zanurzać,
- podgrzewać do temperatury przekraczającej 100 stopni C (212 stopni F),
- naprawiać ani demontować.

Należy wymienić tylko na części zatwierdzone przez IBM. Akumulator należy przetworzyć wtórnie lub usunąć zgodnie z miejscowymi przepisami. W Stanach Zjednoczonych IBM zajmuje się zbieraniem takich akumulatorów. Aby uzyskać więcej informacji, zadzwoń pod numer 1-800-426-4333. Przed zadzwonieniem należy przygotować numer części IBM właściwy dla akumulatora. (C003)



UWAGA: Dotyczy używania dostarczonego przez IBM PODNOŚNIKA sprzedawanego przez inną firmę:

- PODNOŚNIK może być obsługiwany wyłącznie przez autoryzowany personel.
- PODNOŚNIK jest przeznaczony do pomocy przy podnoszeniu, instalowaniu i wyjmowaniu modułów (ładunku) w wysokich stelażach. Nie należy go używać do przewożenia ładunku po pochylniach ani wykorzystywać zamiast podnośników palet czy różnego rodzaju wózków widłowych (ręcznych oraz mechanicznych) w działaniach związanych z przemieszczaniem modułów. W przypadku braku możliwości użycia takich urządzeń należy skorzystać z pomocy odpowiednio wyszkolonego personelu lub ze specjalistycznych usług (np. serwisu montażowego czy transportowego).
- Przed użyciem PODNOŚNIKA należy dokładnie przeczytać i zrozumieć treść podręcznika obsługi. Nieprzeczytanie lub niezrozumienie podręcznika obsługi, a także nieprzestrzeganie zasad bezpieczeństwa i niestosowanie się do instrukcji może spowodować uszkodzenie mienia i/lub obrażenia ciała. W przypadku jakichkolwiek pytań należy skontaktować się z serwisem sprzedawcy urządzenia. Lokalny papierowy podręcznik obsługi musi być zawsze przechowywany razem z urządzeniem, w przeznaczonym do tego pokrowcu. Najnowsza wersja podręcznika obsługi jest dostępna w serwisie WWW sprzedawcy.
- Przed każdorazowym użyciem należy sprawdzić poprawność działania funkcji hamulca stabilizującego. Nie należy na siłę przesuwać ani przetaczać PODNOŚNIKA z zablokowanym hamulcem stabilizującym.
- Nie należy podnosić, opuszczać ani przesuwać platformy załadowniczej, jeśli stabilizator (pedał hamulca) nie jest dobrze zablokowany. W czasie użytkowania i przemieszczania PODNOŚNIKA hamulec stabilizujący musi być stale zablokowany.
- Nie należy przemieszczać PODNOŚNIKA z podniesioną platformą (poza drobnymi korektami ustawienia).
- Nie należy przekraczać maksymalnego dopuszczalnego obciążenia. Maksymalne dopuszczalne obciążenia na środku i na brzegach wysuniętej platformy można odczytać z TABELI DOPUSZCZALNEGO OBCIĄŻENIA.

- Podnosić można wyłącznie ładunek znajdujący się na środku platformy. Nie należy umieszczać na brzegu platformy ładunków przekraczających 91 kg (200 funtów). Należy o tym pamiętać w przypadku obsługi ładunków o przesuniętym środku ciężkości.
- Nie należy obciążać narożnika platformy, systemu zmiany nachylenia, pochylni do umieszczania ładunków ani innych tego rodzaju opcji. Takie platformy – systemy zmiany nachylenia, pochylnie itp. – należy przed użyciem zamocować do głównej półki lub podnośnika widłowego we wszystkich czterech (lub wszystkich innych przewidzianych) miejscach przy użyciu wyłącznie akcesoriów dostarczonych do tego celu. Dopuszczalne ładunki zostały zaprojektowane w taki sposób, aby można je było łatwo zsunąć z platformy bez używania nadmiernej siły. Nie należy więc zbyt mocno pchać ładunków ani się o nie opierać. System zmiany nachylenia powinien być zawsze wypoziomowany, poza drobnymi korektami końcowymi (jeśli będą potrzebne).
- Nie należy stawiać bezpośrednio pod podniesionym ładunkiem
- Nie należy używać PODNOŚNIKA na nierównym podłożu ani na podłożu nachylnym (pochylniach).
- Nie należy układać ładunków w stos.
- Zabrania się obsługi PODNOŚNIKA osobom pozostającym pod wpływem narkotyków lub alkoholu.
- Nie należy opierać o PODNOŚNIK żadnych drabin (chyba że osoba wykonująca zatwierdzone procedury na wysokości z użyciem PODNOŚNIKA uzyskała specjalną zgodę).
- Zagrożenie przewróceniem. Nie należy pchać ładunku ani opierać się o niego przy podniesionej platformie.
- Nie należy używać PODNOŚNIKA jako platformy do podnoszenia osób lub jako stopnia pomocniczego. Nie należy za pomocą PODNOŚNIKA nikogo przewozić.
- Nie należy stawiać na żadnym elemencie PODNOŚNIKA. Nie należy używać platformy jako stopnia pomocniczego.
- Nie należy wdrapywać się na maszt PODNOŚNIKA.
- Nie wolno używać PODNOŚNIKA, jeśli jest uszkodzony lub działa nieprawidłowo.
- Pod platformą występuje ryzyko zmiążdżenia lub przygniecenia. Ładunki należy opuszczać wyłącznie w obszarach wolnych od innych osób i wszelkich przeszkód. Podczas używania PODNOŚNIKA należy trzymać dłonie i stopy poza zasięgiem działania urządzenia.
- Nie wolno używać podnośników widłowych. Nigdy nie należy podnosić ani przemieszczać PODNOŚNIKA za pomocą wózka widłowego dowolnego typu (ręcznego lub mechanicznego).
- Maszt PODNOŚNIKA wysuwa się powyżej poziomu podniesienia platformy. Należy zawsze pamiętać o wysokości sufitu oraz uważać na koryta kablowe, zraszacze, elementy oświetlenia i inne zamontowane w górze obiekty.
- Nie należy pozostawiać PODNOŚNIKA z podniesionym ładunkiem bez opieki.
- Podczas pracy PODNOŚNIKA należy uważać na dłonie, palce i ubranie.
- Wyciągarkę należy obsługiwać tylko ręcznie. Jeśli nie można łatwo obrócić uchwytu wyciągarki jedną ręką, PODNOŚNIK jest prawdopodobnie przeciążony. Po osiągnięciu skrajnego górnego lub dolnego położenia platformy należy zaprzestać obracania uchwytu wyciągarki. Dalsze kręcenie uchwytem może spowodować oderwanie uchwytu i uszkodzenie kabla. Podczas obniżania platformy (odwijania kabla) należy zawsze trzymać co najmniej jedną dłoń na uchwycie. Przed puszczeniem uchwytu należy zawsze upewnić się, że wyciągarka utrzymuje ładunek w bieżącym położeniu.
- Wypadki związane z wyciągarką mogą powodować poważne obrażenia. Nie wolno wykorzystywać PODNOŚNIKA do przemieszczania osób. Należy się upewnić, że podczas podnoszenia sprzętu słyszalny jest dźwięk przeskakiwania zapadki. Przed puszczeniem uchwytu należy się upewnić, że wyciągarka jest zablokowana w bieżącym położeniu. Przed użyciem wyciągarki należy przeczytać odpowiednią stronę instrukcji. Nie wolno dopuścić do swobodnego odwijania kabla na wyciągarce. Może to spowodować nierówne nawinięcie kabla na bębnie, uszkodzenie kabla, a także poważne obrażenia.

- PODNOŚNIK musi być prawidłowo konserwowany, aby pracownik serwisu IBM mógł go użyć. Przed wykonaniem operacji pracownik IBM sprawdzi stan urządzenia i historię konserwacji. Jeśli stan PODNOŚNIKA nie jest odpowiedni, pracownik ma prawo odmówić jego użycia. (C048)

Informacje dotyczące zasilania i okablowania dla NEBS GR-1089-CORE

Poniższe uwagi mają zastosowanie do serwerów IBM oznaczonych jako zgodne z normą NEBS GR-1089-CORE:

Urządzenie nadaje się do instalacji w:

- ośrodkach telekomunikacji sieciowej;
- lokalizacjach, w których mają zastosowanie przepisy NEC (National Electrical Code).

Wewnątrzbudynkowe porty tego urządzenia przeznaczone są do podłączania wyłącznie wewnątrzbudynkowego lub izolowanego okablowania. Portów wewnątrzbudynkowych tego urządzenia *nie wolno* podłączać galwanicznie do interfejsów łączących się z urządzeniami znajdującymi się na zewnątrz ani z ich okablowaniem. Interfejsy te są przeznaczone do używania wyłącznie w charakterze interfejsów wewnątrzbudynkowych (porty typu 2 lub 4, zgodnie z opisem w GR-1089-CORE) i wymagają izolacji odstosowanego okablowania OSP. Dodanie ochronników głównych nie zapewnia wystarczającej ochrony pozwalającej podłączyć te interfejsy galwanicznie do okablowania OSP.

Uwaga: Wszystkie kable ethernetowe muszą być osłonięte i uziemione na obu końcach.

System zasilany prądem przemiennym nie wymaga zastosowania zewnętrznego urządzenia przeciwprzepięciowego.

System zasilany prądem stałym wykorzystuje izolowany przewód ujemny. Ujemnego przewodu akumulatora *nie można* podłączać do obudowy ani uziemienia.

System zasilany prądem stałym jest przeznaczony do instalowania w sieci Common Bonding Network (CBN), zgodnie ze standardem GR-1089-CORE.

Instalowanie i konfigurowanie konsoli HMC

Sekcja zawiera informacje na temat instalowania sprzętu konsoli HMC, podłączania go do systemu zarządzanego oraz konfigurowania do użytku. Czynności te można wykonać we własnym zakresie lub zlecić je dostawcy usług. Dostawca usług może pobrać opłatę za wykonanie usługi.

Co nowego w sekcji Instalowanie i konfigurowanie konsoli HMC

W tym temacie wskazano nowe lub w znacznym stopniu zmienione informacje wprowadzone w sekcji Instalowanie i konfigurowanie konsoli HMC od poprzedniej aktualizacji tej kolekcji tematów.

Kwiecień 2021 r.

- Dodano następujące tematy:
 - [“Instalowanie serwera IBM Power Systems HMC \(7063-CR2\) w stelażu” na stronie 4](#)
 - [“Wymagania wstępne dotyczące instalowania systemów stelażowych 7063-CR2” na stronie 4](#)
 - [“Sprawdzanie zasobów serwera” na stronie 5](#)
 - [“Określanie i oznaczanie położenia w stelażu dla systemu 7063-CR2” na stronie 5](#)
 - [“Mocowanie przewodnic regulowanych do obudowy systemu i do stelaża” na stronie 7](#)
 - [“Mocowanie przewodnic stałych do obudowy systemu i do stelaża” na stronie 8](#)
 - [“Instalowanie serwera w stelażu oraz podłączanie i prowadzenie kabli zasilających” na stronie 10](#)
 - [“Okablowanie stelażowej konsoli HMC 7063-CR2” na stronie 10](#)
 - [“Konfigurowanie konsoli HMC 7063-CR2” na stronie 12](#)

Listopad 2020 r.

- Zaktualizowano następujące tematy:
 - [“Zadania instalowania i konfigurowania” na stronie 2](#)
 - [“Zabezpieczanie konsoli HMC” na stronie 92](#)
 - [“Położenie portów konsoli HMC” na stronie 100](#)

Lipiec 2020 r.

- Zaktualizowano następujące tematy:
 - [“Instalowanie wirtualnego urządzenia konsoli HMC ” na stronie 25](#)
 - [“Położenie portów konsoli HMC” na stronie 100](#)

Październik 2019 r.

- Zaktualizowano następujące tematy:
 - [“Instalowanie wirtualnego urządzenia konsoli HMC ” na stronie 25](#)
 - [“Zabezpieczanie konsoli HMC” na stronie 92](#)

Luty 2019 r.

- Dodano następujące tematy:
 - [“Zabezpieczanie konsoli HMC” na stronie 92](#)
 - [“Rozszerzona strategia hasel” na stronie 94](#)

- [“Rozwiązywanie najczęstszych problemów podczas zabezpieczania konsoli HMC” na stronie 97](#)
- [“Profile zabezpieczeń: RODO i PCI-DSS \(Payment Card Industry Data Security Standard\) ” na stronie 96](#)

Sierpień 2018 r.

- Zaktualizowano następujące tematy:
 - [“Konfigurowanie konsoli HMC 7063-CR1” na stronie 22](#)
 - [“Położenie portów konsoli HMC” na stronie 100](#)

Grudzień 2017 r.

- Dodano informacje na temat serwerów IBM Power Systems z procesorem POWER9.

Zadania instalowania i konfigurowania

Sekcja zawiera informacje na temat czynności związanych z różnymi zadaniami instalowania i konfigurowania konsoli HMC.

W sekcji opisano ogólnie czynności, które muszą zostać wykonane podczas instalowania i konfigurowania konsoli HMC. Konsolę HMC można zainstalować i skonfigurować na różne sposoby. Należy użyć zadania najlepiej pasującego do czynności, która ma zostać wykonana.

Uwagi:

- Do zarządzania serwerami opartymi na procesorach POWER9 należy użyć konsoli HMC w wersji 9.1.0 lub nowszej. Więcej informacji na ten temat zawiera sekcja [“Określanie wersji i wydania kodu maszynowego konsoli HMC” na stronie 81](#).
- Konsola HMC (Hardware Management Console) w wersji 9.2.950 i nowszej nie jest obsługiwana w konsoli HMC 7042 Machine Type. Informacje na temat wersji HMC dla 7042 zawierają uwagi do wydania dostępne w serwisie [Fix Central](#).

Instalowanie i konfigurowanie nowej konsoli HMC z nowym serwerem

Sekcja zawiera informacje ogólne na temat czynności, które muszą zostać wykonane podczas instalowania i konfigurowania nowej konsoli HMC z nowym serwerem.

<i>Tabela 1. Czynności, które muszą zostać wykonane podczas instalowania i konfigurowania nowej konsoli HMC z nowym serwerem</i>	
Czynność	Gdzie znaleźć informacje pokrewne
1. Zbierz informacje i wykonaj czynności opisane w arkuszu konfiguracji wstępnej.	“Arkusz konfiguracji wstępnej dla konsoli HMC” na stronie 50 “Przygotowanie do konfigurowania konsoli HMC” na stronie 49
2. Rozpakuj sprzęt.	
3. Okabluj sprzęt konsoli HMC.	“Okablowanie stelażowej konsoli HMC 7063-CR1” na stronie 20
4. Włącz konsolę HMC przez naciśnięcie przycisku zasilania.	
5. Zaloguj się i uruchom aplikację WWW konsoli HMC.	

Tabela 1. Czynności, które muszą zostać wykonane podczas instalowania i konfigurowania nowej konsoli HMC z nowym serwerem (kontynuacja)

Czynność	Gdzie znaleźć informacje pokrewne
6. Uzyskaj dostęp do Kreatora instalacji z przewodnikiem lub użyj menu konsoli HMC do skonfigurowania konsoli HMC.	“Konfigurowanie konsoli HMC za pomocą Kreatora instalacji z przewodnikiem” na stronie 58 “Konfigurowanie konsoli HMC za pomocą menu ” na stronie 58
7. Podłącz serwer do konsoli HMC.	

Aktualizowanie kodu konsoli HMC

Sekcja zawiera informacje ogólne na temat czynności, które muszą zostać wykonane podczas aktualizowania kodu konsoli HMC.

Jeśli użytkownik ma istniejącą konsolę HMC i chce zaktualizować jej kod, powinien wykonać następujące czynności ogólne.

Tabela 2. Czynności, które muszą zostać wykonane podczas aktualizowania kodu konsoli HMC

Czynność	Gdzie znaleźć informacje pokrewne
1. Uzyskaj aktualizację.	“Aktualizowanie oprogramowania konsoli HMC do nowej wersji” na stronie 86
2. Wyświetl aktualną wersję kodu maszynowego konsoli HMC.	
3. Utwórz kopię zapasową danych profilu systemu zarządzanego.	
4. Utwórz kopię zapasową danych konsoli HMC.	
5. Zapisz bieżące dane konfiguracyjne konsoli HMC.	
6. Zapisz status komend zdalnych.	
7. Zapisz dane aktualizacji.	
8. Zaktualizuj oprogramowanie konsoli HMC do nowej wersji.	
9. Sprawdź, czy aktualizacja kodu maszynowego konsoli HMC została pomyślnie zainstalowana.	

Dodawanie drugiej konsoli HMC do istniejącej instalacji

Sekcja zawiera informacje ogólne na temat czynności, które muszą zostać wykonane podczas dodawania drugiej konsoli HMC do systemu zarządzanego.

Jeśli użytkownik ma już konsolę HMC oraz system zarządzany i chce dodać do tej konfiguracji drugą konsolę HMC, powinien wykonać następujące kroki:

Tabela 3. Czynności, które muszą zostać wykonane podczas dodawania drugiej konsoli HMC do istniejącej instalacji

Czynność	Gdzie znaleźć informacje pokrewne
1. Sprawdź, czy kod konsoli HMC w wersji 7 jest obsługiwany przez sprzęt konsoli HMC.	

Tabela 3. Czynności, które muszą zostać wykonane podczas dodawania drugiej konsoli HMC do istniejącej instalacji (kontynuacja)

Czynność	Gdzie znaleźć informacje pokrewne
2. Zbierz informacje i wykonaj czynności opisane w arkuszu roboczym konfiguracji przed instalacją.	“Arkusz konfiguracji wstępnej dla konsoli HMC” na stronie 50
3. Rozpakuj sprzęt.	
4. Okabluj sprzęt konsoli HMC.	“Okablowanie stelażowej konsoli HMC 7063-CR1” na stronie 20
5. Włącz konsolę HMC przez naciśnięcie przycisku zasilania.	
6. Zaloguj się do konsoli HMC.	
7. Wersje kodu konsoli HMC muszą być zgodne. W razie potrzeby zmień kod na jednej z konsol HMC, aby zapewnić tę zgodność.	“Określanie wersji i wydania kodu maszynowego konsoli HMC” na stronie 81 “Aktualizowanie oprogramowania konsoli HMC do nowej wersji” na stronie 86
8. Uzyskaj dostęp do Kreatora instalacji z przewodnikiem lub użyj menu konsoli HMC do skonfigurowania konsoli HMC.	“Konfigurowanie konsoli HMC za pomocą menu” na stronie 58
9. Skonfiguruj tę konsolę HMC na potrzeby funkcji serwisowych za pomocą Kreatora konfiguracji zgłoszeń automatycznych.	“Konfigurowanie połączenia konsoli HMC z działem serwisu i wsparcia za pomocą kreatora konfiguracji zgłoszeń automatycznych” na stronie 73
10. Podłącz serwer do konsoli HMC.	

Instalowanie konsoli HMC

Przed skonfigurowaniem oprogramowania konsoli HMC należy zainstalować jej sprzęt. Rozdział zawiera informacje na temat instalowania wolnostojącej lub stelażowej konsoli HMC.

Instalowanie serwera IBM Power Systems HMC (7063-CR2) w stelażu

Sekcja zawiera informacje na temat instalowania serwera IBM Power Systems HMC (7063-CR2) w stelażu.

Dokumentację dotyczącą instalowania można wyświetlić w formie elektronicznej lub wydrukować wersję PDF tych samych informacji. Aby wyświetlić lub wydrukować wersję PDF, należy zapoznać się z sekcją [Instalowanie i konfigurowanie konsoli HMC](#).

Wymagania wstępne dotyczące instalowania systemów stelażowych 7063-CR2

Informacje podane w tej sekcji pozwalają na sprawdzenie wymagań wstępnych, których spełnienie jest niezbędne do zainstalowania systemu.

O tym zadaniu



UWAGA: Ta część lub jednostka jest ciężka, ale waży mniej niż 18 kg (39,7 funta). Należy zachować ostrożność podczas podnoszenia, wymontowywania lub montowania tej części lub jednostki. (C008)

Przed rozpoczęciem instalowania serwera może być konieczne zapoznanie się z następującymi dokumentami:

- Najnowsza wersja tego dokumentu jest dostępna w wersji elektronicznej w serwisie WWW [Instalowanie 7063-CR2 w stelażu](http://www.ibm.com/support/knowledgecenter/POWER9/p9hai/p9hai_install7063cr2_kickoff.htm) (http://www.ibm.com/support/knowledgecenter/POWER9/p9hai/p9hai_install7063cr2_kickoff.htm).
- Aby zaplanować instalację serwera, zapoznaj się z sekcją [Planowanie siedziby i sprzętu](#).

Procedura

1. Przed rozpoczęciem instalacji upewnij się, że masz:

- wkrętek krzyżowy, rozmiar 2,
- wkrętek płaski,
- wkrętek T25,
- nóż do kartonu,
- pasek antystatyczny,
- stelaż z przestrzenią na jedną jednostkę EIA (1U).

Uwagi:

- Jeśli nie masz zainstalowanego stelaża, zainstaluj go. Odpowiednie instrukcje zawiera sekcja [Stelaże i opcje stelaży](#) (http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_9xx_kickoff.htm).
 - Parametry zasilacza: 100 - 127 V AC, 9 A (x2), 200 - 240 V AC, 4,5 A (x2); 50 lub 60 Hz.
2. Wykonaj czynności opisane w sekcji [“Sprawdzanie zasobów serwera”](#) na stronie 5.

Sprawdzanie zasobów serwera

Te informacje umożliwiają sprawdzenie zasobów dla systemu.

Procedura

1. Sprawdź, czy zostały dostarczone wszystkie zamówione części.
2. W razie potrzeby rozpakuj komponenty serwera.
3. Przed zainstalowaniem każdego komponentu serwera sprawdź stan części i upewnij się, że wszystkie zamówione części zostały dostarczone.

Uwaga:

Informacje o zamówieniu zostały dołączone do produktu. Informacje o zamówieniu można również uzyskać od przedstawiciela ds. marketingu lub Partnera Handlowego IBM.

Jeśli brakuje części lub są one niepoprawne bądź uszkodzone, skorzystaj z następujących możliwości:

- skontaktuj się z resellerem IBM,
 - zadzwoń na automatyczną linię informacyjną dotyczącą produkcji IBM Rochester pod numerem 1-800-300-8751 (tylko Stany Zjednoczone).
 - odwiedź serwis WWW [Directory of worldwide contacts website](http://www.ibm.com/planetwide) (<http://www.ibm.com/planetwide>); wybierz swoją lokalizację, aby wyświetlić informacje kontaktowe serwisu i wsparcia.
4. Wykonaj czynności opisane w sekcji [“Określanie i oznaczanie położenia w stelażu dla systemu 7063-CR2”](#) na stronie 5.

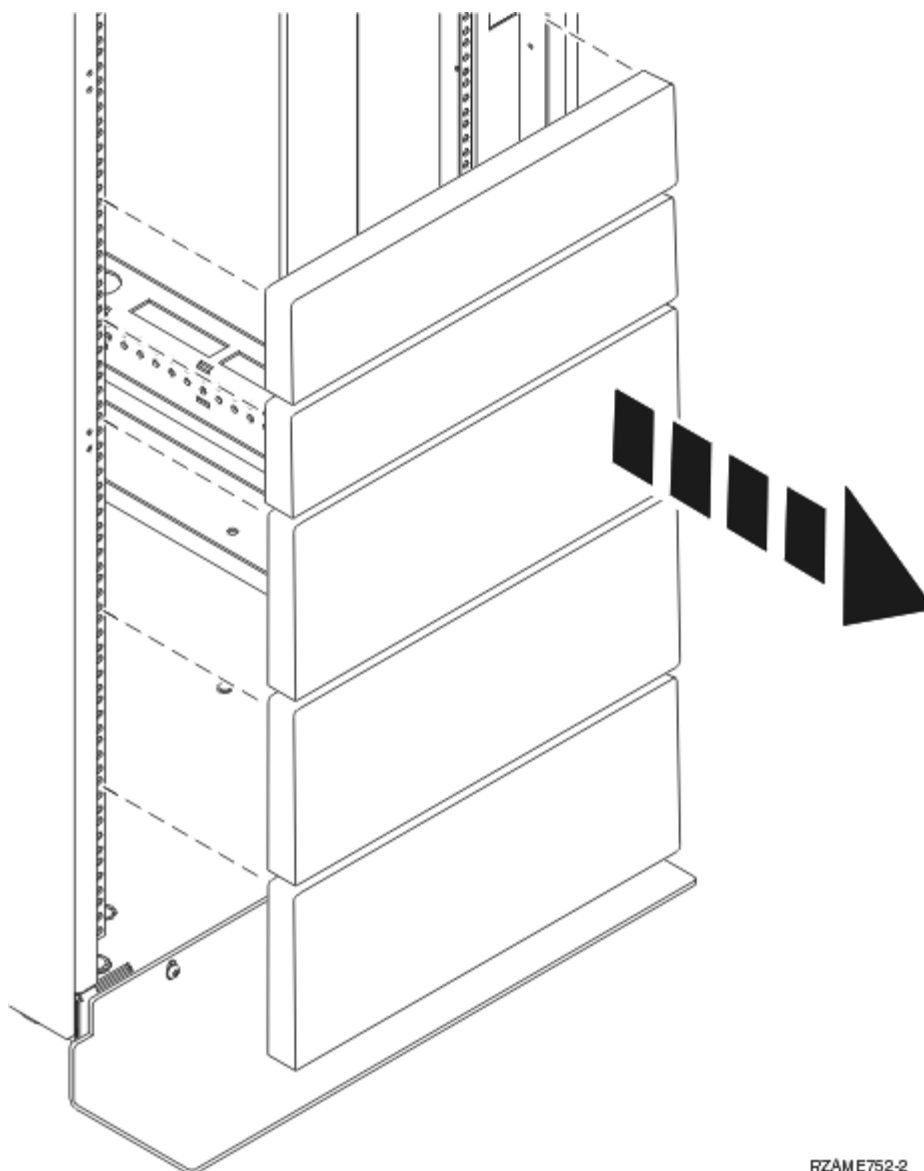
Określanie i oznaczanie położenia w stelażu dla systemu 7063-CR2

Konieczne jest określenie miejsca, w którym jednostka systemowa ma zostać zainstalowana w stelażu.

Procedura

1. Zapoznaj się z tematem [Uwagi dotyczące bezpieczeństwa stelaża](#) (http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_racksafety.htm).

2. Określ położenie jednostki systemowej w stelażu. Planując instalację jednostki systemowej w stelażu, weź pod uwagę następujące informacje:
 - Większe i cięższe jednostki należy umieścić w niższej części stelaża.
 - Zaplanuj w pierwszej kolejności instalację jednostek systemowych w niższej części stelaża.
 - Zapisz w planie poszczególne położenia EIA (Electronic Industries Alliance).
3. Jeśli to konieczne, usuń panele wypełniające, aby uzyskać dostęp do wnętrza stelaża, w którym ma zostać zainstalowana jednostka (Rysunek 1 na stronie 6).



RZAME752-2

Rysunek 1. Usuwanie paneli wypełniających

4. Określ docelowe położenie systemu w stelażu. Zapisz położenie EIA.
5. Patrząc na przód stelaża, z jego prawej strony zaznacz taśmą, markerem lub ołówkiem dolny otwór dla każdej jednostki EIA.
6. Powtórz krok "5" na stronie 6 dla odpowiednich otworów po lewej stronie stelaża.
7. Przejdź do tylnej części stelaża.
8. Z prawej strony znajdź jednostkę EIA, która odpowiada dolnej jednostce EIA oznaczonej z przodu stelaża.
9. Oznacz dolną jednostkę EIA.
10. Oznacz odpowiednie otwory po lewej stronie stelaża.

11. Przejdź do sekcji “Mocowanie prowadnic regulowanych do obudowy systemu i do stelaża” na stronie 7, aby przymocować regulowane prowadnice lub przejdź do sekcji “Mocowanie prowadnic stałych do obudowy systemu i do stelaża” na stronie 8, aby zamocować stałe prowadnice.

Mocowanie prowadnic regulowanych do obudowy systemu i do stelaża

Użytkownik musi zainstalować prowadnice na obudowie i w stelażu. Należy to wykonać zgodnie z niniejszą procedurą.

O tym zadaniu



Ostrzeżenie: Aby uniknąć uszkodzenia prowadnic i nie narażać na zagrożenie siebie ani jednostki, upewnij się, że masz odpowiednie prowadnice i osprzęt dla stelaża. Jeśli otwory w uchwycie montażowym stelaża są kwadratowe lub gwintowane, upewnij się, że prowadnice i osprzęt pasują do otworów uchwytów montażowych używanych w stelażu. Nie należy instalować niepasującego sprzętu z użyciem podkładek lub wypełniaczy. Jeśli nie masz odpowiednich prowadnic i osprzętu dla danego stelaża, skontaktuj się z resellerem IBM.

Uwaga: W stelażach stosowana jest jednostka EIA, która odnosi się do pionowej wysokości 44,45 mm (1,75 cala). Każda wysokość o wartości 44,45 mm (1,75 cala) jest nazywana jednostką EIA. W niektórych krajach ta sama wysokość jest nazywana jednostką U.

Uwaga: System wymaga przestrzeni w stelażu równej jednej jednostce EIA (1U).

Należy upewnić się, że są dostępne wszystkie części niezbędne do zainstalowania prowadnic. Zestaw prowadnic zawiera następujące części:

- 4 - wkręty Philips 6,35 mm (0,25 cala)
- 2 - zespoły prowadnic stelażowych
- 2 - prowadnice wysuwane HMC
- 10 - koszyczki nakrętek dla prostokątnych otworów mocujących EIA
- 10 - koszyczki nakrętek dla okrągłych otworów mocujących EIA
- 10 - wkręty M5 z łbem sześciokątnym i kołnierzem

Procedura

1. Wyjmij części prowadnic z opakowania i umieść je na powierzchni roboczej.
2. Zidentyfikuj obszar 1U w stelażu konsoli HMC.
3. Aby podłączyć prowadnice wysuwane do konsoli HMC, wykonaj następujące czynności:
 - a. Zidentyfikuj prawą prowadnicę wysuwaną.
 - b. Wyrównaj otwory prawej prowadnicy wysuwanej z bolcami prowadnicy wysuwanej znajdującymi się po prawej stronie konsoli HMC. Upewnij się, że wszystkie bolce są wyrównane z otworami.
 - c. Popchnij prowadnicę wysuwaną konsoli HMC do tyłu konsoli HMC, aż do jej pełnego zablokowania na pozycji.
 - d. Zablokuj prawą prowadnicę wysuwaną na prawej stronie konsoli HMC, dokręcając dwa wkręty Philips 6,35 mm (0,25 cala).
 - e. Powtórz kroki “3.a” na stronie 7 - “3.d” na stronie 7, aby zainstalować lewą prowadnicę wysuwaną na lewej stronie konsoli HMC.
4. Przejdź do przedniej części stelaża.
 - a. Po lewej stronie zainstaluj trzy koszyczki dla nakrętki w otworach na przedniej krawędzi stelaża na pozycji 1U przeznaczonej dla konsoli HMC.

Uwaga: Zestaw montażowy zawiera koszyczki dla otworów okrągłych i prostokątnych. Upewnij się, że używane są odpowiednie koszyczki, które są zgodne z otworami w stelażu.
 - b. Powtórz krok “4.a” na stronie 7 dla prawej strony stelaża.

5. Przejdź do tylnej części stelaża.

- a. Po lewej stronie zainstaluj dwa koszyczki dla nakrętki w otworach na przedniej krawędzi stelaża na pozycji 1U przeznaczonej dla konsoli HMC.

Uwaga: Środkowy otwór musi pozostać pusty.

- b. Powtórz krok [“5.a”](#) na stronie 8 dla prawej strony stelaża.

6. Aby zainstalować prowadnice wysuwane konsoli HMC w stelażu, wykonaj następujące czynności:

- a. Zmierz głębokość stelaża. Głębokość musi się mieścić w przedziale od 558,8 mm (22 cale) do 863,6 mm (34 cale).
- b. Umieść prowadnice wysuwane konsoli HMC na płaskiej powierzchni i zlokalizuj wstępnie zainstalowane wkręty.

Uwaga: Prowadnice wysuwane mają cztery otwory gwintowane.

- c. Poluzuj wstępnie zainstalowane wkręty na prowadnicach wysuwanych na tyle, aby prowadnice mogły być łatwo wsuwane i wysuwane.
- d. W zależności od głębokości stelaża mierzonej w kroku [“6.a”](#) na stronie 8 należy dopasować wkręty na prowadnicach.
 - i) Jeśli głębokość stelaża mieści się w zakresie od 558,8 mm (22 cale) do 698,5 mm (27,5 cala), przykręć wkręty do pierwszego i trzeciego otworu.
 - ii) Jeśli głębokość stelaża mieści się w zakresie od 698,5 mm (27,5 cala) do 863,6 mm (34 cale), przykręć wkręty do drugiego i czwartego otworu.

Uwagi:

- Pierwszym otworem jest zawsze otwór położony najbliżej końca prowadnicy wysuwanej. Otwory trzeci i czwarty są umieszczone bliżej siebie.
- Upewnij się, że wkręty są wystarczająco poluzowane, tak aby długość prowadnicy wysuwanej mogła być dostosowana podczas instalowania w stelażu.

7. W przedniej części stelaża zainstaluj prowadnice konsoli HMC, wykonując następujące kroki:

- a. Znajdź zespół lewej prowadnicy.
- b. Przykręć zespół prowadnicy tak, aby koniec z najbliższym otworem gwintowym (pierwszy otwór) wchodził do stelaża jako pierwszy. Upewnij się, że nakrętki są skierowane do wnętrza stelaża. Otwarta szczelina zespołu prowadnicy znajduje się najbliżej przedniej części stelaża.
- c. Po lewej stronie stelaża podłącz uchwyt montażowy na końcu prowadnicy do przedniej krawędzi stelaża, używając dwóch wkrętów M5, pozostawiając wolny otwór środkowy. Upewnij się, że zespół prowadnic jest poluzowany z przodu stelaża, aby umożliwić włożenie konsoli HMC.

8. Z tyłu stelaża po prawej stronie pociągnij za wolny koniec prowadnicy do tyłu i przymocuj uchwyt montażowy do stelaża za pomocą dwóch wkrętów M5, pozostawiając wolny otwór środkowy.

9. Powtórz krok [“7”](#) na stronie 8 i krok [“8”](#) na stronie 8, aby zainstalować prawy zespół prowadnicy po prawej stronie stelaża.

10. Zainstaluj stację roboczą konsoli HMC od przodu stelaża, wykonując następujące czynności:

- a. Trzymając stację roboczą konsoli HMC poziomo, włóż wewnętrzne prowadnice do prowadnic konsoli HMC, które zostały zainstalowane w poprzednim kroku. Wciśnij konsolę HMC, aż uchwyty z przodu konsoli HMC będą wyrównane z gwintowanymi otworami w przedniej części stelaża.
- b. Podłącz konsolę HMC do lewej strony ramy za pomocą jednego wkrętu M5. Powtórz ten krok po prawej stronie stelaża.

11. Wykonaj czynności opisane w sekcji [“Instalowanie serwera w stelażu oraz podłączanie i prowadzenie kabli zasilających”](#) na stronie 10.

Mocowanie prowadnic stałych do obudowy systemu i do stelaża

Użytkownik musi zainstalować prowadnice na obudowie i w stelażu. Należy to wykonać zgodnie z niniejszą procedurą.

O tym zadaniu



Ostrzeżenie: Aby uniknąć uszkodzenia prowadnic i nie narażać na zagrożenie siebie ani jednostki, upewnij się, że masz odpowiednie prowadnice i osprzęt dla stelaża. Jeśli otwory w uchwycie montażowym stelaża są kwadratowe lub gwintowane, upewnij się, że prowadnice i osprzęt pasują do otworów uchwytów montażowych używanych w stelażu. Nie należy instalować niepasującego sprzętu z użyciem podkładek lub wypełniaczy. Jeśli nie masz odpowiednich prowadnic i osprzętu dla danego stelaża, skontaktuj się z resellerem IBM.

Uwaga: W stelażach stosowana jest jednostka EIA, która odnosi się do pionowej wysokości 44,45 mm (1,75 cala). Każda wysokość o wartości 44,45 mm (1,75 cala) jest nazywana jednostką EIA. W niektórych krajach ta sama wysokość jest nazywana jednostką U.

Uwaga: System wymaga przestrzeni w stelażu równej jednej jednostce EIA (1U).

Należy upewnić się, że są dostępne wszystkie części niezbędne do zainstalowania prowadnic. Zestaw prowadnic zawiera następujące części:

- 4 - wkręty Philips 6,35 mm (0,25 cala)
- 2 - prowadnice wewnętrzne
- 2 - prowadnice HMC
- 2 - koszyczki nakrętek dla prostokątnych otworów mocujących EIA
- 2 - koszyczki nakrętek dla okrągłych otworów mocujących EIA
- 8 - wkręty M5 z łbem sześciokątnym i kołnierzem

Procedura

1. Wyjmij części prowadnic z opakowania i umieść je na powierzchni roboczej.
2. Zidentyfikuj obszar 1U w stelażu konsoli HMC.
3. Aby podłączyć prowadnice wewnętrzne do konsoli HMC, wykonaj następujące czynności:
 - a. Zidentyfikuj prawą prowadnicę wewnętrzną.
 - b. Wyrównaj otwory prawej wewnętrznej prowadnicy z bolcami prowadnicy wewnętrznej znajdującymi się po prawej stronie konsoli HMC. Upewnij się, że wszystkie bolce są wyrównane z otworami.
 - c. Popchnij wewnętrzną prowadnicę konsoli HMC do przodu konsoli HMC, aż do jej pełnego zablokowania na pozycji.
 - d. Zablokuj prawą wewnętrzną prowadnicę na prawej stronie konsoli HMC, dokręcając dwa wkręty Philips 6,35 mm (0,25 cala).
 - e. Powtórz kroki 3.a - "3.d" na stronie 9, aby zainstalować lewą wewnętrzną prowadnicę po lewej stronie konsoli HMC.
4. Przejdź do przedniej części stelaża. Po lewej stronie zainstaluj jeden koszyczek dla nakrętki w otworze na przedniej krawędzi stelaża na pozycji 1U przeznaczonej dla konsoli HMC.

Uwaga: Zestaw montażowy zawiera koszyczki dla otworów okrągłych i prostokątnych. Upewnij się, że używane są odpowiednie koszyczki, które są zgodne z otworami w stelażu.
5. Przejdź do tylnej części stelaża. Po lewej stronie zainstaluj jeden koszyczek dla nakrętki w środkowym otworze na przedniej krawędzi stelaża na pozycji 1U przeznaczonej dla konsoli HMC.
6. W przedniej części stelaża zainstaluj prowadnice konsoli HMC, wykonując następujące kroki:
 - a. Wyrównaj bolce prowadnic nad i pod koszyczkiem nakrętki zainstalowanym w poprzednim kroku.
 - b. Po prawej stronie stelaża podłącz uchwyt montażowy na końcu prowadnicy do przedniej krawędzi stelaża, używając dwóch wkrętów M5, do górnych i dolnych otworów gwintowanych, pozostawiając wolny otwór środkowy. Upewnij się, że zespół prowadnic jest poluzowany z przodu stelaża, aby umożliwić włożenie konsoli HMC.
7. Z tyłu stelaża po prawej stronie pociągnij za wolny koniec prowadnicy do tyłu i przymocuj uchwyt montażowy do stelaża za pomocą dwóch wkrętów M5, pozostawiając wolny otwór środkowy.

8. Powtórz krok "6" na stronie 9 i krok "7" na stronie 9, aby zainstalować lewy zespół prowadnicy po lewej stronie stelaża.
 9. Zainstaluj stację roboczą konsoli HMC od przodu stelaża, wykonując następujące czynności:
 - a. Trzymając stację roboczą konsoli HMC poziomo, włóż wewnętrzne prowadnice do prowadnic konsoli HMC, które zostały zainstalowane w poprzednim kroku. Wciśnij konsolę HMC, aż uchwyty z przodu konsoli HMC będą wyrównane z gwintowanymi otworami w przedniej części stelaża.
 - b. Podłącz konsolę HMC do lewej strony ramy za pomocą jednego wkrętu M5. Powtórz ten krok po prawej stronie stelaża.
- Uwaga:** Usuń pomarańczowe wsporniki transportowe, jeśli zostały przymocowane z tyłu systemu, następnie ponownie wkręć wkręt.
10. Wykonaj czynności opisane w sekcji "Instalowanie serwera w stelażu oraz podłączanie i prowadzenie kabli zasilających" na stronie 10.

Instalowanie serwera w stelażu oraz podłączanie i prowadzenie kabli zasilających

Sekcja zawiera informacje na temat instalowania systemu na prowadnicach oraz podłączania i prowadzenia kabli zasilających.

O tym zadaniu

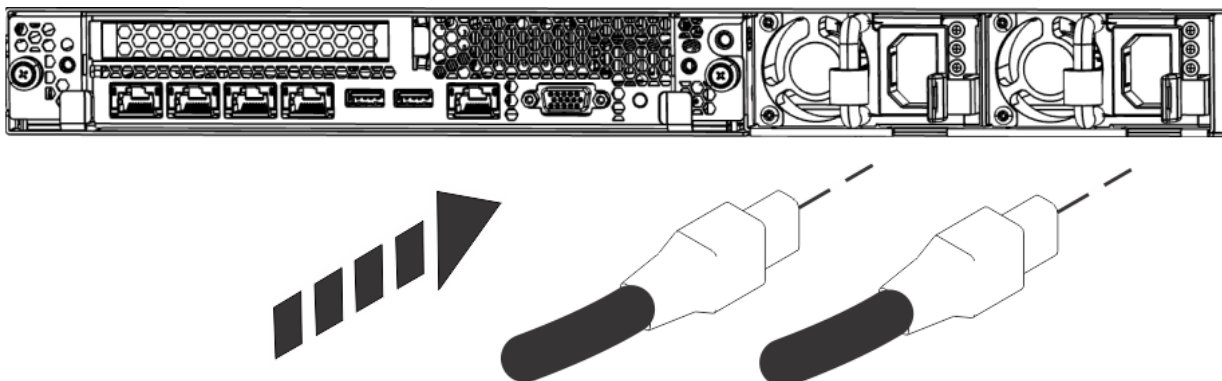


UWAGA: Ta część lub jednostka jest ciężka, ale waży mniej niż 18 kg (39,7 funta). Należy zachować ostrożność podczas podnoszenia, wymontowywania lub montowania tej części lub jednostki. (C008)

Procedura

1. Usuń plastikową taśmę ochronną z górnej części obudowy systemu.
2. Podłącz kable zasilające do zasilaczy.

Uwaga: Nie podłączaj teraz drugiego końca kabla zasilającego do źródła zasilania.



Rysunek 2. Podłączanie kabli zasilających do zasilaczy

3. Zapnij zapięcia rzepowe, aby zabezpieczyć kable zasilające.
4. Wykonaj czynności opisane w sekcji "Okablowanie stelażowej konsoli HMC 7063-CR2" na stronie 10.

Okablowanie stelażowej konsoli HMC 7063-CR2

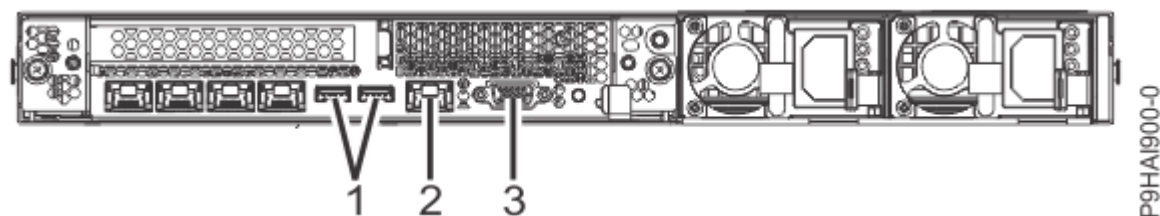
Sekcja zawiera opis fizycznej instalacji stelażowej konsoli HMC.

Procedura

1. Upewnij się, że konsola HMC jest zainstalowana w stelażu, a kable zasilające są podłączone do zasilaczy. Więcej informacji zawiera sekcja "Instalowanie serwera w stelażu oraz podłączanie i

przewodzenie kabli zasilających” na stronie 10. Po zainstalowaniu konsoli HMC w stelażu przejdź do następnego kroku.

2. Podłącz klawiaturę, monitor i mysz.

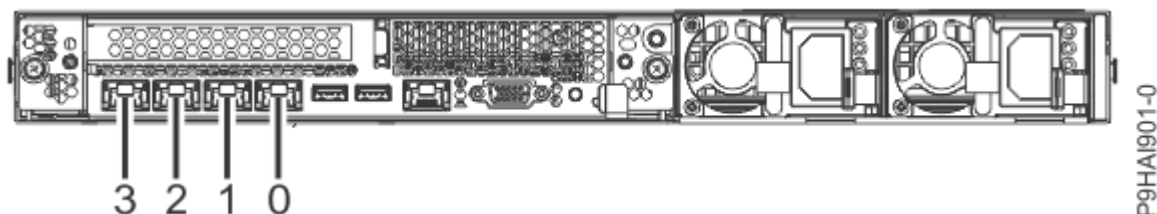


Rysunek 3. Porty z tyłu

Tabela 4. Porty wejściowe i wyjściowe	
Identyfikator	Opis
1	Port USB 2.0 używany do podłączenia klawiatury i myszy
2	Port IPMI (Ethernet Intelligent Platform Management Interface)
3	Port VGA (Video Graphics Array) używany do podłączenia monitora. Obsługiwane jest tylko ustawienie VGA 1024 x 768 przy częstotliwości 60 Hz. Obsługiwany jest tylko kabel o maksymalnej długości 3 metrów.

Uwaga: Serwer ma z przodu dwa porty USB, których można używać.

3. Podłącz port Ethernet interfejsu IPMI do sieci.



Rysunek 4. Porty Ethernet

Tabela 5. Porty Ethernet	
Identyfikator	Opis
0	Współużytkowany interfejs IPMI (Ethernet Intelligent Platform Management Interface) i połączenie sieciowe konsoli HMC
1, 2 i 3	Połączenie sieciowe konsoli HMC

Uwaga: To połączenie jest wymagane do uzyskania dostępu do kontrolera BMC (baseboard management controller) na konsoli HMC. Dostęp do konsoli BMC jest wymagany do wykonywania zadań serwisowych i aktualizacji oprogramowania wbudowanego konsoli HMC. Więcej informacji na ten temat zawiera sekcja “Typy połączeń sieciowych konsoli HMC” na stronie 41.

Ostrzeżenie: Na terenie Twojego kraju produkt ten mógł nie być objęty certyfikacją w zakresie połączeń, za pomocą dowolnych środków, do interfejsów publicznych sieci telekomunikacyjnych. Proces certyfikacji dotyczący takich połączeń może być wymagany przepisami prawa w okresie późniejszym. Aby uzyskać więcej informacji, skontaktuj się z IBM.

4. Podłącz kabel Ethernet przeznaczony do łączenia z systemem zarządzanym lub z serwerami.

Uwagi:

- Jeśli używane jest połączenie współużytkowane dla interfejsu IPMI i konsoli HMC, jeden kabel podłączony do portu 0 na rysunku 2 może spełnić oba wymagania dla interfejsu IPMI i konsoli HMC.
 - Więcej informacji na temat połączeń sieciowych konsoli HMC zawiera sekcja [“Połączenia sieciowe konsoli HMC”](#) na stronie 40.
5. Jeśli system zarządzany jest już zainstalowany, można sprawdzić aktywność kablowego połączenia ethernetowego przez obserwację zielonych kontrolki statusu przy portach sieci Ethernet konsoli HMC i systemu zarządzanego w miarę postępu instalowania konsoli.
6. Podłącz kable zasilające serwera oraz kable zasilające wszystkich innych podłączonych urządzeń do źródła zasilania prądem przemiennym (AC).
7. Sprawdź status zasilania za pomocą kontrolki zasilacza. Więcej informacji na ten temat zawiera sekcja [Kontrolki w systemie 7063-CR2](#).
8. Naciśnij przycisk zasilania, aby uruchomić system. Kontrolka zasilania przestaje migać i pozostaje włączona, co oznacza, że zasilanie systemu jest włączone.

Wyniki

W następnej kolejności należy zainstalować i skonfigurować oprogramowanie konsoli HMC. Wykonaj czynności opisane w sekcji [“Konfigurowanie konsoli HMC 7063-CR2”](#) na stronie 12.

Konfigurowanie konsoli HMC 7063-CR2

Sekcja zawiera informacje na temat instalowania i konfigurowania konsoli HMC (Hardware Management Console).

Sprawdź dostarczoną wersję konsoli HMC. Aby dowiedzieć się, w jaki sposób wyświetlić wersję i wydanie kodu maszynowego konsoli HMC, należy zapoznać się z sekcją [Sprawdź dostarczoną wersję konsoli HMC](#). Najnowszą wersję konsoli HMC można pobrać z serwisu [WWW Fix Central](#). Należy utworzyć startowy plik ISO na podstawie pakietu konsoli HMC (obraz ISO) znajdującego się na nośniku wymiennym (takim jak DVD lub USB).

Uwaga: W poniższej tabeli opisano predefiniowane (domyślne) informacje logowania dla interfejsów konsoli HMC i kontrolera BMC.

Tabela 6.			
Konsola lub interfejs	Domyślny identyfikator	Domyślne hasło	Opis
BMC (OpenBMC)	root	0penBmc	Identyfikator i hasło użytkownika root są używane do pierwszego zalogowania się do kontrolera BMC.
HMC	hscroot	abc123	Identyfikator i hasło użytkownika hscroot są używane do pierwszego zalogowania się do konsoli HMC. Wielkość liter w identyfikatorze i hasle jest rozróżniana. Identyfikator i hasło mogą być używane tylko przez użytkownika mającego przypisaną rolę głównego administratora.

Tabela 6. (kontynuacja)			
Konsola lub interfejs	Domyślny identyfikator	Domyślne hasło	Opis
HMC	root	passw0rd	Identyfikator i hasło użytkownika root są używane przez dostawcę usług do przeprowadzenia procedur obsługi technicznej. Nie można ich używać do logowania się do konsoli HMC.

Uwaga: Poniżej przedstawiono przykładowe instalacje.

Instalowanie konsoli HMC przy użyciu dysku flash USB

Aby zainstalować konsolę HMC z dysku flash USB, wykonaj następujące kroki w systemach Linux®:

Uwaga: Przykłady dla różnych systemów operacyjnych:

- Windows: [Nośniki instalacyjne flash USB \(Windows\)](#)
- Mac: [Nośniki instalacyjne flash USB \(macOS\)](#)

1. Pobierz pożądaną wersję konsoli HMC z serwisu [WWW Fix Central](#).
2. Uruchom następującą komendę: **dd bs=4M if=/ścieżka/do/PLIKU_ISO_HMC.iso of=/dev/sdx status=progress && sync** (gdzie **sdx** to nazwa dysku USB).

Uwaga: W systemie Linux można użyć komendy `lsblk` w celu określenia nazwy urządzenia podłączonego dysku USB.

3. Włóż dysk USB i włącz system.

Uwaga: Dysk USB musi mieć pojemność co najmniej 8 GB. Niektóre napędy USB mogą być zbyt szerokie, aby można je było poprawnie włożyć do portu USB w tylnej części systemu. Przed przejściem dalej sprawdź, czy dysk USB pasuje.

4. Po wyświetleniu menu Petitboot wybierz opcję **Install Hardware Management Console** (Zainstaluj konsolę HMC) znajdującą się poniżej urządzenia **USB**.

Instalowanie konsoli HMC przy użyciu nośnika wirtualnego z poziomu BMC

Aby zainstalować konsolę HMC przy użyciu nośnika wirtualnego z poziomu BMC, wykonaj następujące kroki:

1. Otwórz obsługiwaną przeglądarkę WWW. Na pasku adresu wprowadź adres IP konsoli BMC, z którą ma zostać nawiązane połączenie. Na przykład można użyć formatu `https://<IP BMC>`.
2. W oknie **OpenBMC logon** (Logowanie do konsoli OpenBMC) wprowadź adres **hosta** BMC oraz wypełnij pola **Username** (Nazwa użytkownika) i **Password** (Hasło).

Uwaga: Domyślnym identyfikatorem użytkownika jest `root`, a domyślnym hasłem jest `OpenBmc`.

Jeśli używany jest poziom oprogramowania wbudowanego OP940.01 lub wyższy, hasło użytkownika `root` jest domyślnie przedawnione. Przed uzyskaniem dostępu do konsoli BMC należy zmienić hasło domyślne. Więcej informacji na temat zmiany domyślnego hasła, które utraciło ważność, zawiera sekcja [Ustawianie hasła](#).

Jeśli zapomniałeś hasła, możesz zresetować system do ustawień fabrycznych, aby przywrócić domyślne hasło. Aby zresetować system, należy zapoznać się z sekcją [Resetowanie do ustawień fabrycznych](#).

3. Kliknij przycisk **Log in** (Zaloguj się).

4. Wybierz opcję **Server control** (Sterowanie serwerem).
5. Wybierz opcję **Virtual Media** (Nośnik wirtualny).
6. Kliknij przycisk **Choose file** (Wybierz plik).
7. Znajdź plik ISO nośnika odtwarzania konsoli HMC i kliknij opcję **Open** (Otwórz).
8. Kliknij przycisk **Start** (Uruchom).
9. Włącz system.
10. Po wyświetleniu menu Petitboot wybierz opcję **Install Hardware Management Console** (Zainstaluj konsolę HMC) znajdującą się poniżej urządzenia **USB**.

Instalowanie konsoli HMC z użyciem zewnętrznego dysku DVD podłączonego do portu USB

Aby zainstalować konsolę HMC z użyciem zewnętrznego dysku DVD podłączonego do portu USB, wykonaj następujące kroki:

1. Pobierz pożądaną wersję obrazu odtwarzania konsoli HMC z serwisu [WWW Fix Central](#).
2. Zapisz obraz DVD odtwarzania konsoli HMC na nośniku DVD-R DL.
3. Wyłącz konsolę HMC.
4. Podłącz zewnętrzny napęd DVD ze złączem USB do konsoli HMC i włóż dysk DVD odtwarzania konsoli HMC.

Uwaga: Może zająć konieczność podłączenia napędu DVD ze złączem USB do zewnętrznego źródła zasilania lub użycia rozdzielacza USB w celu podłączenia go do dodatkowego portu USB, aby zapewnić napędowi DVD wystarczające zasilanie.

5. Włącz konsolę HMC.

Uwaga: Podczas uruchamiania ekran monitora może być ciemny. Wyświetlenie na ekranie monitora jakiegokolwiek statusu może nastąpić dopiero po 2 lub 3 minutach.

6. Po uruchomieniu programu ładującego Petitboot należy przejść do opcji zatrzymania startu automatycznego.

Uwaga: Wymuszany jest 10-sekundowy limit czasu. Jeśli w czasie 10 sekund nie zostanie podjęte żadne działanie, system spróbuje wystartować z dysku twardego.

7. Zaczekaj, aż w menu Petitboot zostanie wyświetlone urządzenie **CD/DVD**.

Uwaga: Ten proces może zająć około minuty.

8. Wybierz opcję **Install Hardware Management Console** (Zainstaluj konsolę HMC) znajdującą się pod urządzeniem **CD/DVD**.

Instalowanie systemu 7063-CR1 w stelażu

Sekcja zawiera informacje na temat sposobu instalowania konsoli HMC 7063-CR1 w stelażu.

Dokumentację dotyczącą instalowania można wyświetlić w formie elektronicznej lub wydrukować wersję PDF tych samych informacji. Aby wyświetlić lub wydrukować wersję PDF, należy zapoznać się z sekcją [Instalowanie i konfigurowanie konsoli HMC](#).

Wymagania wstępne dotyczące instalowania systemów stelażowych 7063-CR1

Informacje podane w tej sekcji pozwalają na sprawdzenie wymagań wstępnych, których spełnienie jest niezbędne do zainstalowania systemu.

O tym zadaniu

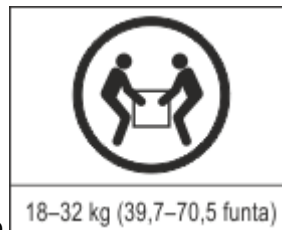


UWAGA:

lub



lub



Waga tej części lub jednostki wynosi od 18 do 32 kg (od 39,7 do 70,5 funta). Aby bezpiecznie podnieść tę część lub jednostkę, konieczne są dwie osoby. (C009)

Przed rozpoczęciem instalowania serwera może być konieczne zapoznanie się z następującymi dokumentami:

- Najnowsza wersja tego dokumentu jest dostępna w wersji elektronicznej w serwisie WWW [Instalowanie 7063-CR1 w stelażu](http://www.ibm.com/support/knowledgecenter/POWER9/p9hai/p9hai_install7063_kickoff.htm) (http://www.ibm.com/support/knowledgecenter/POWER9/p9hai/p9hai_install7063_kickoff.htm).
- Aby zaplanować instalację serwera, zapoznaj się z sekcją [Planowanie siedziby i sprzętu](#).

Procedura

Przed rozpoczęciem instalacji upewnij się, że masz:

- wkrętak krzyżowy, rozmiar 2,
- wkrętak płaski,
- nóż do kartonu,
- pasek antystatyczny,
- stelaż z przestrzenią na jedną jednostkę EIA (1U).

Uwaga: Jeśli nie masz zainstalowanego stelaża, zainstaluj go. Odpowiednie instrukcje zawiera sekcja [Stelaże i opcje stelaży](http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_9xx_kickoff.htm) (http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_9xx_kickoff.htm).

Sprawdzanie zasobów serwera

Te informacje umożliwiają sprawdzenie zasobów dla systemu.

Procedura

1. Sprawdź, czy zostały dostarczone wszystkie zamówione części.
2. W razie potrzeby rozpakuj komponenty serwera.
3. Przed zainstalowaniem każdego komponentu serwera sprawdź stan części i upewnij się, że wszystkie zamówione części zostały dostarczone.

Uwaga:

Informacje o zamówieniu zostały dołączone do produktu. Informacje o zamówieniu można również uzyskać od przedstawiciela ds. marketingu lub Partnera Handlowego IBM.

Jeśli brakuje części lub są one niepoprawne bądź uszkodzone, skorzystaj z następujących możliwości:

- skontaktuj się z resellerem IBM,
- zadzwoń na automatyczną linię informacyjną dotyczącą produkcji IBM Rochester pod numer 1-800-300-8751 (tylko Stany Zjednoczone),

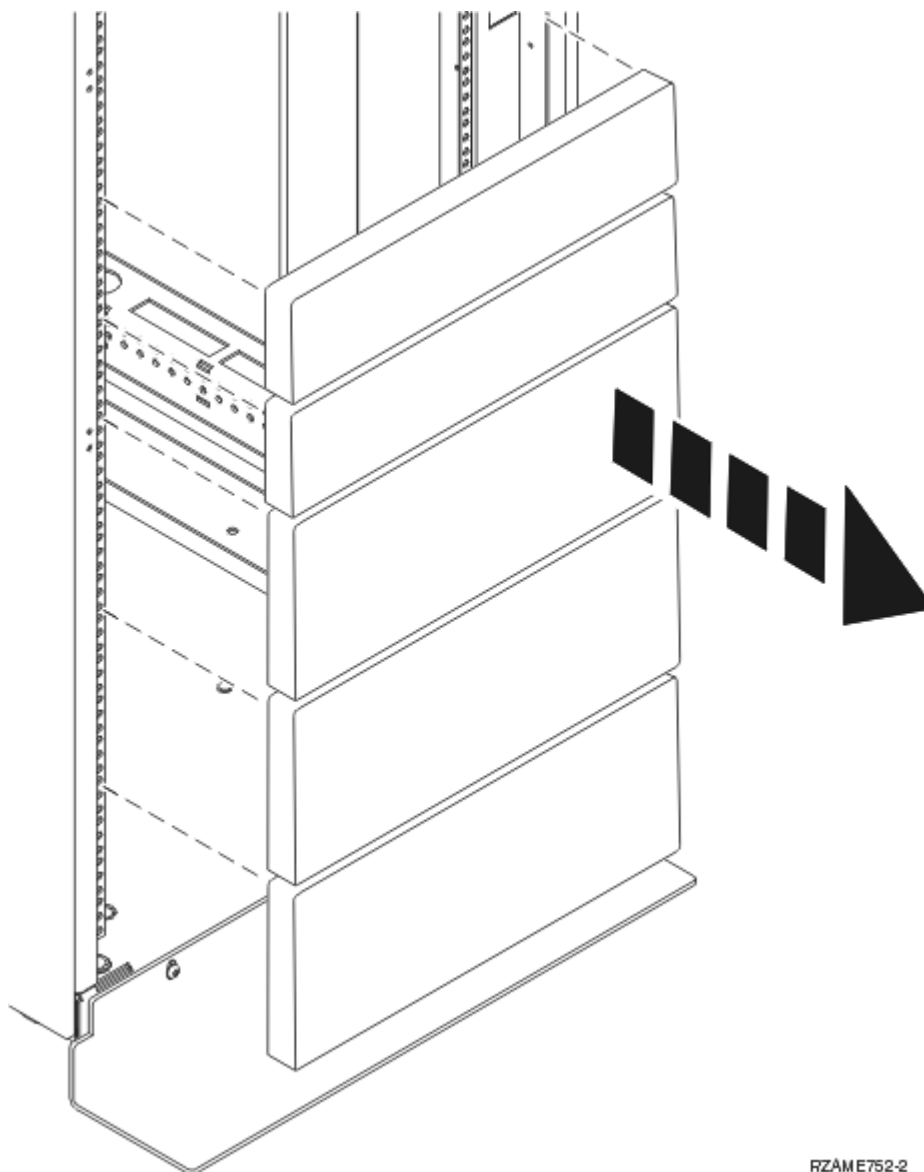
- odwiedź serwis [WWW Directory of worldwide contacts website](http://www.ibm.com/planetwide) (<http://www.ibm.com/planetwide>); wybierz swoją lokalizację, aby wyświetlić informacje kontaktowe serwisu i wsparcia.

Określanie i oznaczanie położenia w stelażu dla systemu 7063-CR1

Może być konieczne określenie miejsca, w którym jednostka systemowa ma zostać zainstalowana w stelażu.

Procedura

1. Zapoznaj się z tematem [Uwagi dotyczące bezpieczeństwa stelaża](http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_racksafety.htm) (http://www.ibm.com/support/knowledgecenter/POWER9/p9hbf/p9hbf_racksafety.htm).
2. Określ położenie jednostki systemowej w stelażu. Planując instalację jednostki systemowej w stelażu, weź pod uwagę następujące informacje:
 - Większe i cięższe jednostki należy umieścić w niższej części stelaża.
 - Zaplanuj w pierwszej kolejności instalację jednostek systemowych w niższej części stelaża.
 - Zapisz w planie poszczególne położenia EIA (Electronic Industries Alliance).
3. Jeśli to konieczne, usuń panele wypełniające, aby uzyskać dostęp do wnętrza stelaża, w którym ma zostać zainstalowana jednostka ([Rysunek 5 na stronie 17](#)).



RZAME752-2

Rysunek 5. Usuwanie paneli wypełniających

4. Określ docelowe położenie systemu w stelażu. Zapisz położenie EIA.
5. Patrząc na przód stelaża, z jego prawej strony zaznacz taśmą, markerem lub ołówkiem dolny otwór dla każdej jednostki EIA.
6. Powtórz krok ["5"](#) na stronie 17 dla odpowiednich otworów po lewej stronie stelaża.
7. Przejdź do tylnej części stelaża.
8. Z prawej strony znajdź jednostkę EIA, która odpowiada dolnej jednostce EIA oznaczonej z przodu stelaża.
9. Oznacz dolną jednostkę EIA.
10. Oznacz odpowiednie otwory po lewej stronie stelaża.

Mocowanie przewodnic stałych do obudowy systemu i do stelaża

Użytkownik musi zainstalować przewodnice na obudowie i w stelażu. Należy to wykonać zgodnie z niniejszą procedurą.

O tym zadaniu



Ostrzeżenie: Aby uniknąć uszkodzenia przewodnic i nie narażać na zagrożenie siebie ani jednostki, upewnij się, że masz odpowiednie przewodnice i osprzęt dla stelaża. Jeśli otwory w uchwycie montażowym stelaża są kwadratowe lub gwintowane, upewnij się, że przewodnice i osprzęt pasują do otworów uchwytów montażowych używanych w stelażu. Nie należy instalować niepasującego sprzętu z użyciem podkładek lub wypełniaczy. Jeśli nie masz odpowiednich przewodnic i osprzętu dla danego stelaża, skontaktuj się z resellerem IBM.

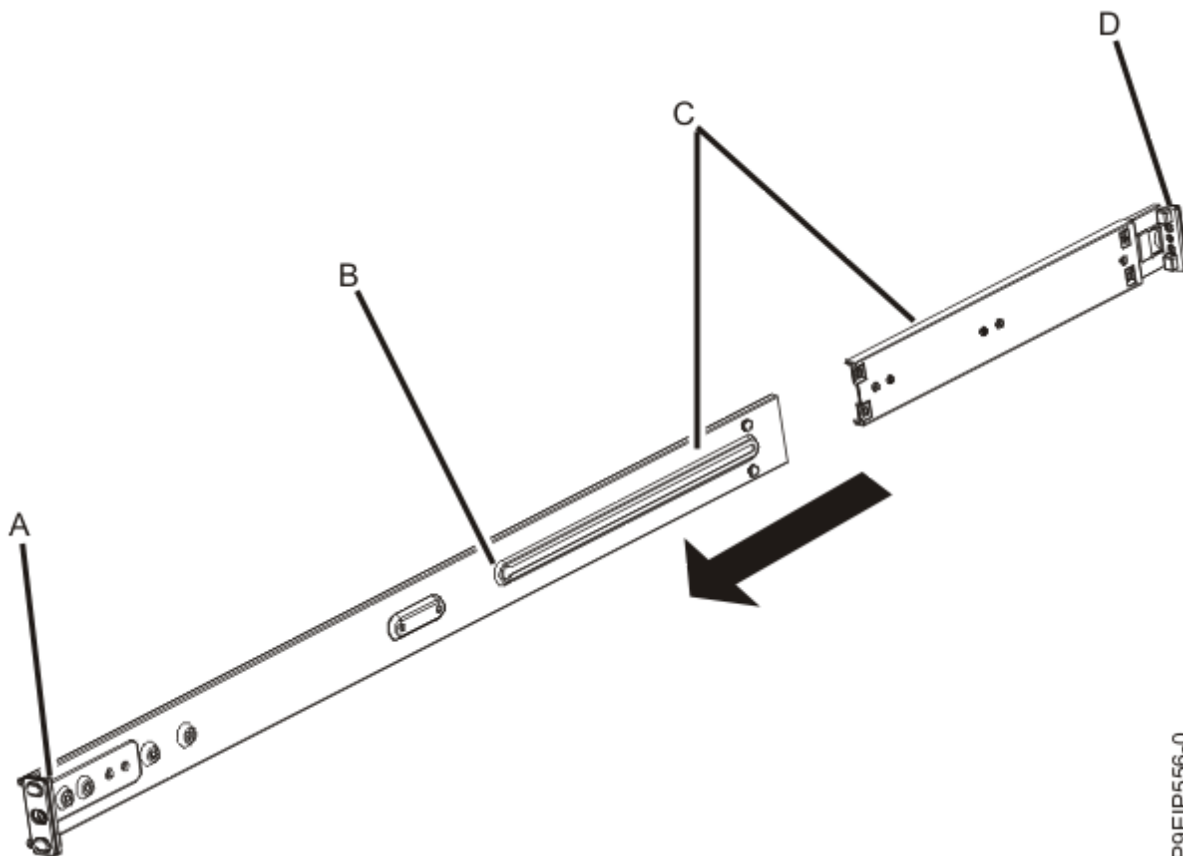
Uwaga: System wymaga przestrzeni w stelażu równej jednej jednostce EIA (1U).

Należy upewnić się, że są dostępne wszystkie części niezbędne do zainstalowania przewodnic. Zestaw przewodnic zawiera następujące części:

- Wkręty przewodnic wysuwanych używane do łączenia dwóch części każdej z przewodnic wysuwanych.
- Wkręty do stelaża dla przewodnic wysuwanych używane do mocowania przewodnic w stelażu.
- Przewodnice.
- Wkręty 10 – 32 x 0,635 cm (0,25 cala) używane do mocowania przewodnic do obudowy systemu.

Procedura

1. Wyjmij części przewodnic z opakowania i umieść je na powierzchni roboczej.
2. Zastąp kwadratowe bolce do stelaża dla przewodnic (**A**) i (**D**) bolcami okrągłymi.
3. Połącz dwie części każdej z przewodnic wysuwanych stelaża. Aby połączyć dwie części przewodnicy wysuwanej stelaża, wykonaj następujące czynności:
 - a. Zidentyfikuj dwie części lewej przewodnicy wysuwanej stelaża. Dopasuj krótkie i długie części (**C**). Upewnij się, że przetyczki stelaża wskazują ten sam kierunek (**A**) i (**D**).



- b. Krótsza część przewodnicy wysuwanej stelaża ma metalowy bolec. Włóż bolec do otworu w dłuższej części przewodnicy wysuwanej stelaża (**B**). Wsuń krótszą część przewodnicy stelaża do dłuższej części przewodnicy stelaża.

P9EIP556-0

- c. Wyrównaj otwory w dwóch częściach prowadnic wysuwanych stelaża. Za pomocą wkrętaka krzyżowego połącz dwie części, luźno wkręcając dwa gwintowane wkręty prowadnicy w otwory w prowadnicy wysuwanej stelaża.

Uwaga: Nie dokręcaj jeszcze wkrętów prowadnicy wysuwanej stelaża.

- d. Powtórz te kroki dla prawej prowadnicy wysuwanej.
4. Zainstaluj prowadnice wysuwane w stelażu.
- a. Przejdź do przedniej części stelaża.
 - b. Wybierz lewą prowadnicę wysuwaną stelaża i znajdź oznaczoną wcześniej jednostkę EIA. Każda prowadnica wysuwana jest oznaczona również słowem **Back** (Tył) w celu wskazania tyłu stelaża. Upewnij się, że trzymasz przedni koniec prowadnicy wysuwanej stelaża.
 - c. Rozszerz prowadnicę od przedniej do tylnej części stelaża i wyrównaj bolce prowadnicy wysuwanej stelaża z wcześniej oznaczonymi otworami w uchwycie stelaża.
 - d. Wsuń przetyczki prowadnicy stelaża do uchwytu tylnej części stelaża aż do zatrzaśnięcia zatrzasku w tylnej części stelaża.
 - e. Pociągnij przód prowadnicy stelaża w kierunku przedniej części uchwytu prowadnicy stelaża. Wyrównaj bolce prowadnicy wysuwanej z otworami w uchwycie prowadnicy i pociągnij, aż do zatrzaśnięcia zatrzasku.
 - f. Za pomocą wkrętaka dokręć wkręty prowadnicy luźno wkręcone w kroku 2.
- Uwaga:** Aby uzyskać dostęp do wkrętów prowadnic i je dokręcić, może być potrzebne miejsce o wysokości 2U.
- g. Powtórz kroki 4a–4f dla prawej prowadnicy wysuwanej.

Instalowanie serwera w stelażu oraz podłączanie i prowadzenie kabli zasilających

Sekcja zawiera informacje na temat instalowania systemu na prowadnicach oraz podłączania i prowadzenia kabli zasilających.

O tym zadaniu

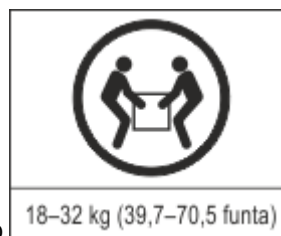


UWAGA:

lub



lub



Waga tej części lub jednostki wynosi od 18 do 32 kg (od 39,7 do 70,5 funta). Aby bezpiecznie podnieść tę część lub jednostkę, konieczne są dwie osoby. (C009)

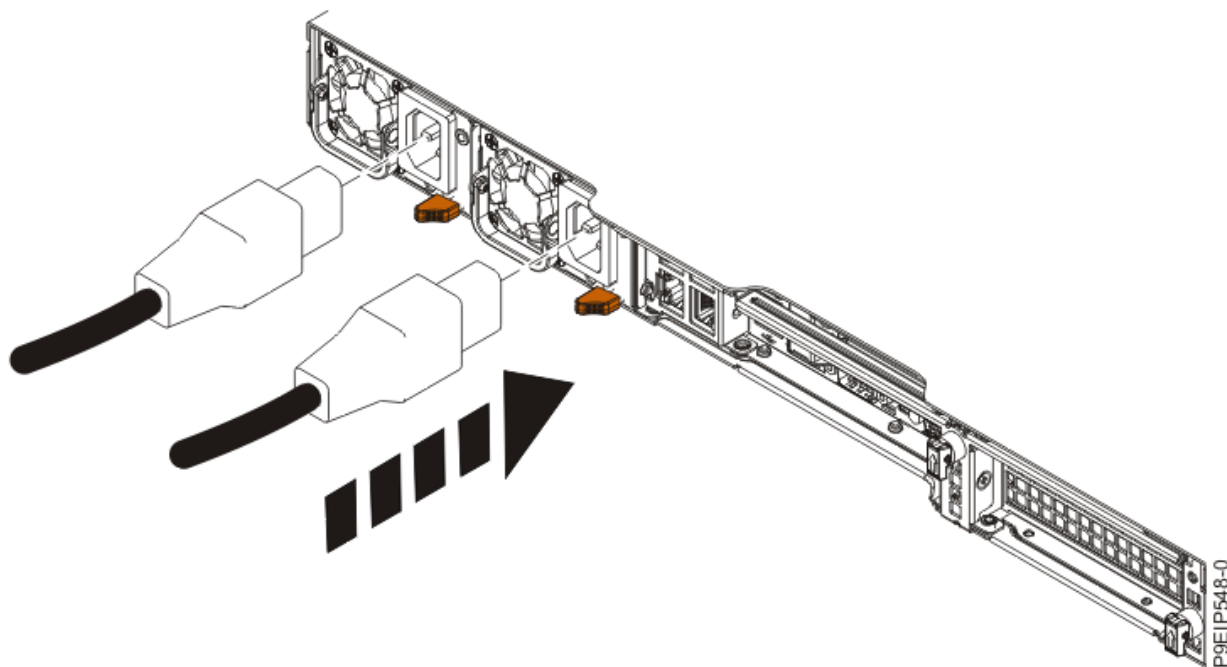
Procedura

1. Usuń plastikową taśmę ochronną z górnej części obudowy systemu.
2. Przejdź do przedniej części stelaża.
3. Z pomocą drugiej osoby (po jednej osobie z każdej strony serwera) podnieś serwer i dopasuj prowadnice po obu stronach obudowy serwera do prowadnic wysuwanych stelaża.
4. Delikatnie wsuń serwer do stelaża w stronę jego tylnej części.
5. Umocuj serwer w stelażu, wkręcając wkręty z podkładkami przez uchwyty po każdej stronie obudowy systemu.

Uwaga: Użycie podkładek z wkrętami jest konieczne. Wsuń podkładkę na każdy z dwóch dłuższych wkrętów (1,5 cm (0,59 cala)) dołączonych do zestawu przewodnic. Wkręć wkręt z podkładką po prawej i lewej stronie z przodu serwera.

6. Podłącz kable zasilające do zasilaczy.

Uwaga: Nie podłączaj teraz drugiego końca kabla zasilającego do źródła zasilania.



Rysunek 6. Podłączanie kabli zasilających do zasilaczy

7. Wykonaj czynności opisane w sekcji [“Okablowanie stelażowej konsoli HMC 7063-CR1”](#) na stronie 20.

Okablowanie stelażowej konsoli HMC 7063-CR1

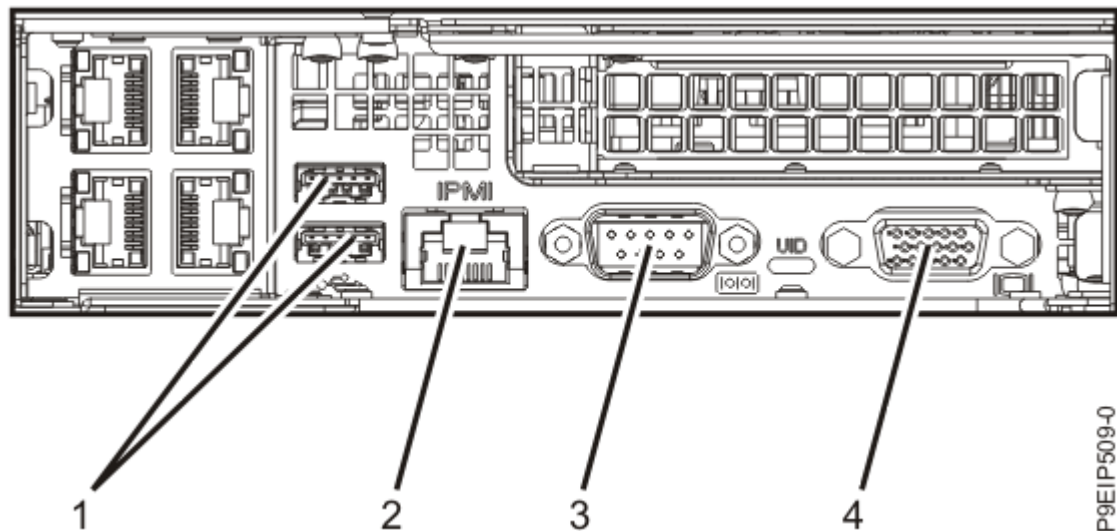
Sekcja zawiera opis fizycznej instalacji stelażowej konsoli HMC.

Procedura

1. Upewnij się, że konsola HMC jest zainstalowana w stelażu, a kable zasilające są podłączone do zasilaczy. Więcej informacji na ten temat zawiera sekcja [“Instalowanie serwera w stelażu oraz podłączanie i prowadzenie kabli zasilających”](#) na stronie 19. Po zainstalowaniu konsoli HMC w stelażu przejdź do następnego kroku.

Uwaga: Jeśli port, który ma być używany w tylnej części systemu, jest zasłonięty wtyczką, usuń ją. Osłony portów gwarantują, że użytkownik będzie pamiętać o zresetowaniu hasła administratora systemu zarządzanego po zakończeniu ładowania programu startowego (IPL) systemu.

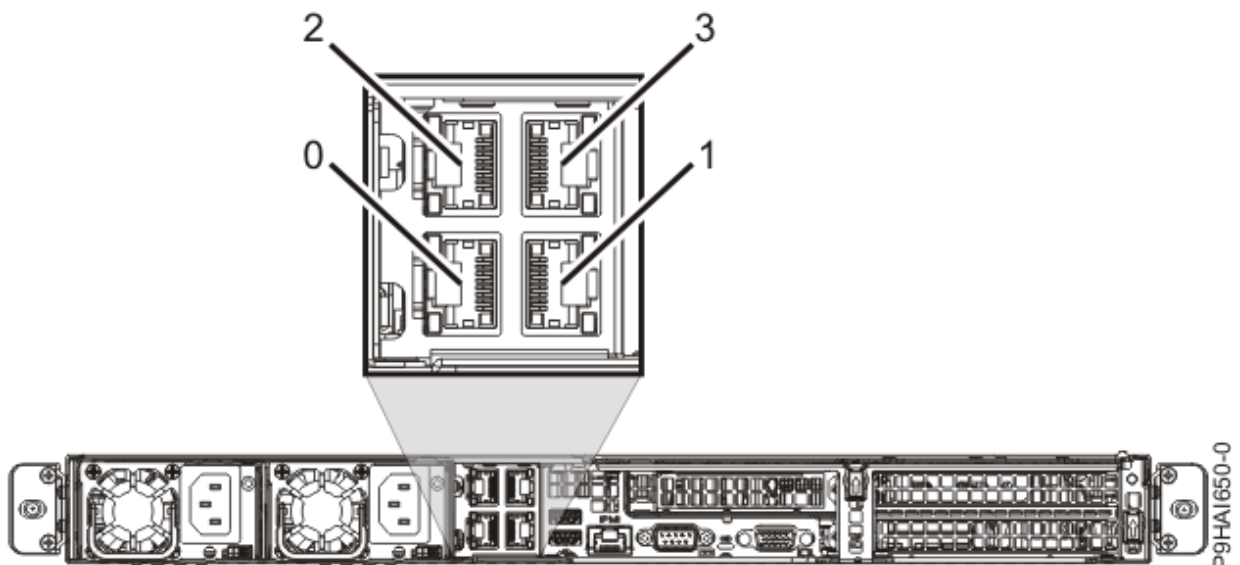
2. Podłącz klawiaturę, monitor i mysz.



Rysunek 7. Porty z tyłu

Tabela 7. Porty wejściowe i wyjściowe	
Identyfikator	Opis
1	Port USB 2.0 używany do podłączenia klawiatury i myszy
2	Port IPMI (Ethernet Intelligent Platform Management Interface)
3	Szeregowy port IPMI
4	Port VGA (Video Graphics Array) używany do podłączenia monitora. Obsługiwane jest tylko ustawienie VGA 1024 x 768 przy częstotliwości 60 Hz. Obsługiwany jest tylko kabel o maksymalnej długości 3 metrów.

Uwaga: Serwer ma z przodu dwa porty USB, których można używać. Przedni port szeregowy nie działa.
3. Podłącz kabel Ethernet przeznaczony do łączenia z systemem zarządzanym lub z serwerami.



Rysunek 8. Porty Ethernet

Uwaga: Więcej informacji na temat połączeń sieciowych konsoli HMC zawiera sekcja [“Połączenia sieciowe konsoli HMC”](#) na stronie 40.

4. Jeśli system zarządzany jest już zainstalowany, można sprawdzić aktywność kablowego połączenia ethernetowego przez obserwację zielonych kontrolек statusu przy portach sieci Ethernet konsoli HMC i systemu zarządzanego w miarę postępu instalowania konsoli.
5. Podłącz port Ethernet interfejsu IPMI do sieci.

Uwaga: To połączenie jest wymagane do uzyskania dostępu do kontrolera BMC (baseboard management controller) na konsoli HMC. Dostęp do konsoli BMC jest wymagany do wykonywania zadań serwisowych i aktualizacji oprogramowania wbudowanego konsoli HMC. Więcej informacji na ten temat zawiera sekcja [“Typy połączeń sieciowych konsoli HMC”](#) na stronie 41.

6. Podłącz kable zasilające serwera oraz kable zasilające wszystkich innych podłączonych urządzeń do źródła zasilania prądem przemiennym (AC).
7. Sprawdź status zasilania za pomocą kontrolек zasilacza. Więcej informacji zawiera sekcja [Kontrolki w systemie 7063-CR1](#)

Wyniki

W następnej kolejności należy zainstalować i skonfigurować oprogramowanie konsoli HMC. Wykonaj czynności opisane w sekcji [“Konfigurowanie konsoli HMC 7063-CR1”](#) na stronie 22.

Konfigurowanie konsoli HMC 7063-CR1

Sekcja zawiera informacje na temat instalowania i konfigurowania konsoli HMC (Hardware Management Console).

Sprawdź dostarczoną wersję konsoli HMC. Najnowszą wersję konsoli HMC można pobrać z serwisu [WWW Fix Central](#). Należy utworzyć startowy plik ISO na podstawie pakietu konsoli HMC (obraz ISO) znajdującego się na nośniku wymiennym (takim jak DVD lub USB).

Uwaga: W poniższej tabeli opisano predefiniowane (domyślne) informacje logowania dla interfejsów konsoli HMC i kontrolera BMC.

Tabela 8.			
Konsola lub interfejs	Domyślny identyfikator	Domyślne hasło	Opis
BMC	ADMIN	ADMIN	Identyfikator i hasło użytkownika ADMIN są używane do pierwszego zalogowania się do kontrolera BMC.
Konsola HMC	hscroot	abc123	Identyfikator i hasło użytkownika hscroot są używane do pierwszego zalogowania się do konsoli HMC. Wielkość liter w identyfikatorze i hasle jest rozróżniana. Identyfikator i hasło mogą być używane tylko przez użytkownika mającego przypisaną rolę głównego administratora.

Tabela 8. (kontynuacja)			
Konsola lub interfejs	Domyślny identyfikator	Domyślne hasło	Opis
Konsola HMC	root	passw0rd	Identyfikator i hasło użytkownika root są używane przez dostawcę usług do przeprowadzenia procedur obsługi technicznej. Nie można ich używać do logowania się do konsoli HMC.

Uwaga: Poniżej przedstawiono przykładowe instalacje.

Instalowanie konsoli HMC przy użyciu dysku flash USB

Aby zainstalować konsolę HMC z dysku flash USB, wykonaj następujące kroki w systemach Linux:

Uwaga: Przykłady dla różnych systemów operacyjnych:

- Windows: [Nośniki instalacyjne flash USB \(Windows\)](#)
- Mac: [Nośniki instalacyjne flash USB \(macOS\)](#)

1. Pobierz pożądaną wersję konsoli HMC z serwisu [WWW Fix Central](#).
2. Uruchom następującą komendę: **dd bs=4M if=/ścieżka/do/PLIKU_ISO_HMC.iso of=/dev/sdx status=progress && sync** (gdzie **sdx** to nazwa dysku USB).

Uwaga: W systemie Linux można użyć komendy `lsblk` w celu określenia nazwy urządzenia podłączonego dysku USB.

3. Włóż dysk USB i włącz system.

Uwaga: Dysk USB musi mieć pojemność co najmniej 4 GB. Niektóre napędy USB mogą być zbyt szerokie, aby można je było poprawnie włożyć do portu USB w tylnej części systemu. Przed przejściem dalej sprawdź, czy dysk USB pasuje.

4. Po wyświetleniu menu Petitboot wybierz opcję **Install Hardware Management Console** (Zainstaluj konsolę HMC) znajdującą się poniżej urządzenia **USB**.

Instalowanie konsoli HMC przy użyciu nośnika zdalnego z poziomu przeglądarki konsoli

Aby zainstalować konsolę HMC przy użyciu nośnika zdalnego z poziomu przeglądarki konsoli, wykonaj następujące kroki:

1. Zaloguj się do interfejsu WWW kontrolera BMC (<http://<bmc-ip>>).
2. Wybierz opcję **Remote Control** (Zdalne sterowanie).
3. Wybierz opcję **Console Redirection** (Przekierowanie konsoli).
4. Kliknij opcję **Launch Console** (Uruchom konsolę).
5. W przeglądarce Java™ iKVM Viewer wybierz kolejno opcje **Virtual Media > Virtual Storage** (Nośnik wirtualny > Wirtualna pamięć masowa).
6. W obszarze **Logical Drive Type** (Typ napędu logicznego) wybierz opcję **ISO File** (Plik ISO).
7. Kliknij opcję **Open Image** (Otwórz obraz) i znajdź plik ISO w systemie.
8. Kliknij przycisk **Plugin** (Podłącz), aby podłączyć plik ISO.
9. Włącz system.

10. Po wyświetleniu menu Petitboot wybierz opcję **Install Hardware Management Console** (Zainstaluj konsolę HMC) znajdującą się poniżej urządzenia **CD/DVD**.

Instalowanie konsoli HMC z użyciem zewnętrznego dysku DVD podłączonego do portu USB

Aby zainstalować konsolę HMC z użyciem zewnętrznego dysku DVD podłączonego do portu USB, wykonaj następujące kroki:

1. Pobierz pożądaną wersję obrazu odtwarzania konsoli HMC z serwisu [WWW Fix Central](http://www.fixcentral.com).
2. Zapisz obraz DVD odtwarzania konsoli HMC na nośniku DVD-R jako obraz. Alternatywnie możesz zamówić nośnik odtwarzania na DVD.
3. Wyłącz konsolę HMC.
4. Podłącz zewnętrzny napęd DVD ze złączem USB do konsoli HMC i włóż dysk DVD odtwarzania konsoli HMC.

Uwaga: Może zająć konieczność podłączenia napędu DVD ze złączem USB do zewnętrznego źródła zasilania lub użycia rozdzielnicy USB w celu podłączenia go do dodatkowego portu USB, aby zapewnić napędowi DVD wystarczające zasilanie.

5. Włącz konsolę HMC.

Uwaga: Podczas uruchamiania ekran monitora może być ciemny. Wyświetlenie na ekranie monitora jakiegokolwiek statusu może nastąpić dopiero po 2 lub 3 minutach.

6. Po uruchomieniu programu ładującego Petitboot należy przejść do opcji zatrzymania startu automatycznego.

Uwaga: Wymuszany jest 10-sekundowy limit czasu. Jeśli w czasie 10 sekund nie zostanie podjęte żadne działanie, system spróbuje wystartować z dysku twardego.

7. Zaczekaj, aż w menu Petitboot zostanie wyświetlone urządzenie **CD/DVD**.

Uwaga: Ten proces może zająć około minuty.

8. Wybierz opcję **Install Hardware Management Console** (Zainstaluj konsolę HMC) znajdującą się pod urządzeniem **CD/DVD**.

Instalowanie konsoli HMC przy użyciu nośnika zdalnego udostępnianego przez serwer plików SMB

Aby zainstalować konsolę HMC przy użyciu nośnika zdalnego, który jest udostępniany przez serwer plików SMB (Server Message Block), wykonaj następujące kroki:

1. Skopiuj plik ISO odtwarzania na host współużytkowania znajdujący się na serwerze plików obsługującym protokół SMB.

Uwaga: Protokół SMBv3 (Server Message Block wersja 3) nie jest obsługiwany.

2. Zaloguj się do interfejsu WWW kontrolera BMC (<http://<bmc-ip>>).
3. Wybierz opcję **Virtual Media** (Nośnik wirtualny).
4. Wybierz opcję **CD-ROM Image** (Obraz CD-ROM).
5. Uzupełnij następujące informacje:

Share host (Host współużytkowania)

Adres IP hosta SMB. Jeśli używana jest nazwa hosta, upewnij się, że system nazw domen (DNS) na kontrolerze BMC został poprawnie skonfigurowany.

Path to image (Ścieżka do obrazu)

Ścieżka SMB do systemu. Na przykład: `/<nazwa współużytkowana>/<pozostała część ścieżki>/<nazwa obrazu ISO>.iso`

User (Użytkownik) – opcjonalnie

Nazwa użytkownika używana do zalogowania się do hosta SMB.

Password (Hasło) – opcjonalnie

Hasło użytkownika.

6. Kliknij przycisk **Save** (Zapisz).
 7. Kliknij opcję **Mount** (Podłącz).
 8. Na urządzeniu 1 zostanie teraz wyświetlony następujący komunikat: **There is an iso file mounted** (Podłączono plik ISO).
- Uwaga:** Jeśli komunikat nie zostanie wyświetlony, ponownie sprawdź podane informacje i powtórz kroki od 6 do 8.
9. Włącz system.
 10. Po wyświetleniu menu Petitboot wybierz opcję **Install Hardware Management Console** (Zainstaluj konsolę HMC) znajdującą się poniżej urządzenia **CD/DVD**.

Opcjonalnie: zaktualizuj poziom oprogramowania wbudowanego konsoli HMC za pomocą dołączonej pamięci USB

Uwaga: Jeśli do konfiguracji dołączono aktualizację oprogramowania wbudowanego w pamięci USB, wykonaj następujące kroki, aby zaktualizować poziom oprogramowania wbudowanego konsoli HMC.

Aby zaktualizować poziom oprogramowania wbudowanego konsoli HMC z użyciem dołączonej pamięci USB, wykonaj następujące kroki:

1. Umieść pamięć USB w porcie USB z tyłu systemu.
2. Włącz system and i zaloguj się do konsoli HMC.
3. W obszarze nawigacyjnym kliknij ikonę **HMC Management** (Zarządzanie konsolą HMC) , a następnie wybierz opcję **Console Management** (Zarządzanie konsolą).
4. W panelu zawartości kliknij opcję **Update the Hardware Management Console** (Aktualizacja konsoli HMC).
5. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie kreatora Install HMC Corrective Service (Instaluj poprawkę konsoli HMC).

W następnej kolejności należy skonfigurować oprogramowanie konsoli HMC. Odpowiednie instrukcje zawiera sekcja [“Konfigurowanie konsoli HMC” na stronie 40](#).

Pojęcia pokrewne

Konfigurowanie połączenia z kontrolerem BMC

Istnieje możliwość wyświetlenia i skonfigurowania ustawień sieciowych kontrolera BMC na potrzeby konsoli zarządzania.

Instalowanie wirtualnego urządzenia konsoli HMC

Sekcja zawiera informacje na temat instalowania wirtualnego urządzenia konsoli Hardware Management Console (HMC).

Wirtualne urządzenie konsoli HMC może być instalowana w ramach istniejącej zwirtualizowanej infrastruktury x86 lub POWER. Wirtualne urządzenie konsoli HMC obsługuje następujące hiperwizory wirtualizacji x86:

- maszyna wirtualna bazująca na jądrze (KVM),
- hiperwizor Xen,
- VMware.

Wirtualne urządzenie konsoli HMC obsługuje następujące hiperwizory wirtualizacji POWER:

- PowerVM

Minimalne wymagania dla uruchomienia wirtualnego urządzenia konsoli HMC:

- 16 GB pamięci,
- 4 procesory wirtualne,
- 2 interfejsy sieciowe (maksymalnie dozwolone 4),
- 1 dysk zawierający 500 GB dostępnego miejsca.

Uwagi:

- System hosta wirtualnego urządzenia konsoli HMC musi być wyposażony w procesor Intel VT-x lub AMD-V z obsługą wirtualizacji sprzętowej.
- Otrzymywane przez użytkownika nośniki DVD wirtualnego urządzenia konsoli HMC nie są nośnikami startowymi. Należy najpierw podłączyć nośnik, a następnie skopiować z niego plik .tgz. Metoda podłączania nośnika DVD może się różnić w zależności od używanego systemu operacyjnego.
- Składnia komendy wykorzystana w następujących przykładach może się różnić w zależności od używanego systemu operacyjnego.
- Hiperwizor wirtualizacji PowerVM wymaga 160 GB miejsca na dysku. Jednakże zalecane jest 500 GB pamięci.
- Minimalne wymagania dotyczące procesora PowerVM to 1,0 jednostki przetwarzającej i cztery współużytkowane procesory wirtualne w trybie współużytkowania limitowanego. Nie jest zalecane korzystanie z procesorów dedykowanych. Procesor PowerVM wymaga również 16 GB pamięci.

Informacje pokrewne

[Obrazy instalacji sieciowej konsoli HMC 8 oraz instrukcje instalacji](#)

Instalowanie wirtualnego urządzenia konsoli HMC w środowisku o architekturze x86

Sekcja zawiera informacje na temat instalowania wirtualnego urządzenia konsoli Hardware Management Console (HMC) w środowisku o architekturze x86.

Instalowanie wirtualnego urządzenia konsoli HMC przy użyciu hiperwizora KVM

Sekcja zawiera informacje na temat instalowania wirtualnego urządzenia konsoli Hardware Management Console (HMC) przy użyciu hiperwizora maszyny wirtualnej bazującej na jądrze (KVM).

Aby zainstalować konsolę wirtualne urządzenie konsoli HMC na maszynie KVM, wykonaj następujące kroki:

Uwaga: Następujące czynności są wykonywane z interfejsu wiersza komend i wymagają uprawnień administratora. Składnia komendy może się różnić w zależności od systemu operacyjnego.

1. Sprawdź, czy pakiety wirtualizacji są zainstalowane w serwerach z systemem operacyjnym Red Hat Enterprise Linux (RHEL) w wersji 7.0 lub nowszej.
2. Pobierz plik <nazwa_pliku_instalacyjnego_vHMC_dla_KVM>.tar.gz do systemu hosta.
3. Uruchom następującą komendę: `mkdir -p /var/lib/libvirt/images/vHMC`.
4. Uruchom następującą komendę: `cd /var/lib/libvirt/images/vHMC`.
5. Aby wyodrębnić obrazy dysków wirtualnych, uruchom następującą komendę: `tar -zxvf <nazwa_pliku_instalacyjnego_vHMC_dla_KVM>.tgz`

Uwaga: W tej komendzie należy podać pełną ścieżkę do pliku .tar wirtualnego urządzenia konsoli HMC.

6. W archiwum <nazwa_pliku_instalacyjnego_vHMC_dla_KVM>.tar.gz znajduje się plik **domain.xml**. Wykonaj następujące kroki:

- a. Otwórz plik **domain.xml** do edycji i sprawdź, czy ścieżki dysków są poprawne. Plik zawiera łańcuch **DISK_PATH**.
 - b. Upewnij się, że wartość magistrali dotycząca urządzenia dysku zawiera nazwę **virtio**.
 - c. Maszynie wirtualnej można nadać inną nazwę. Nazwą domyślną w pliku **domain.xml** jest **vHMC**.
 - d. Sprawdź, czy w pliku **domain.xml** jest ustawiony adres MAC. Plik zawiera łańcuch **MAC_ADDRESS**.
- Uwaga:** Usuń ten wiersz, jeśli adres MAC ma być generowany automatycznie.
- e. Sprawdź zgodność mostów z urządzeniami Ethernet. W domyślnym pliku **domain.xml** podano jedno urządzenie Ethernet.
 - f. Jeśli używany jest mechanizm aktywacji, zastąp wartość **AEDISK** nazwą obrazu dysku wirtualnego mechanizmu aktywacji. W przeciwnym razie usuń element dotyczący dysku.
7. Aby zdefiniować maszynę wirtualną, uruchom następującą komendę: `virsh define <domena>.xml`.
 8. Aby sprawdzić, czy wirtualna konsola HMC została dodana do listy zdefiniowanych maszyn wirtualnych, uruchom następującą komendę: `virsh list --all`.
 9. Aby uruchomić maszynę wirtualną, uruchom następującą komendę: `virsh start vHMC`.
 10. Aby określić numer terminala VNC (Virtual Network Computing) używanej konsoli, uruchom następującą komendę: `virsh vncdisplay vHMC`.
 11. Aby połączyć się z konsolą przy użyciu przeglądarki VNC, uruchom następującą komendę: `vncviewer NAZWA_HOSTA:ID` (gdzie ID to numer ekranu, na przykład 0).
- Uwaga:** Jeśli jest konieczny dostęp zdalny, należy wyłączyć firewall lub skonfigurować go tak, aby zezwalał na dostęp do portu 5900.

Instalowanie wirtualnego urządzenia konsoli HMC w środowisku hiperwizora Xen

Sekcja zawiera informacje na temat instalowania wirtualnego urządzenia konsoli Hardware Management Console (HMC) w środowisku hiperwizora Xen.

Wirtualne urządzenie konsoli HMC obsługuje hiperwizor Xen w wersji 4.2 lub późniejszej.

Aby zainstalować wirtualne urządzenie konsoli HMC przy użyciu hiperwizora Xen, wykonaj następujące kroki:

Uwaga: Następujące kroki są wykonywane z interfejsu wiersza komend i wymagają uprawnień administratora. Składnia komendy może się różnić w zależności od systemu operacyjnego.

1. Sprawdź, czy pakiety wirtualizacji są zainstalowane w serwerach z systemem operacyjnym Red Hat Enterprise Linux (RHEL) w wersji 6.4 lub późniejszej.
2. Pobierz plik `<nazwa_pliku_instalacyjnego_vHMC_dla_XEN>.tar.gz` do systemu hosta.
3. Uruchom następującą komendę: `mkdir -p /var/lib/libvirt/images/vHMC`.
4. Uruchom następującą komendę: `cd /var/lib/libvirt/images/vHMC`.
5. Aby wyodrębnić obrazy dysków wirtualnych, uruchom następującą komendę: `tar -zxvf <nazwa_pliku_instalacyjnego_vHMC_dla_XEN>.tgz`

Uwaga: W tej komendzie należy podać pełną ścieżkę do pliku `.tar` wirtualnego urządzenia konsoli HMC.

6. W archiwum `<nazwa_pliku_instalacyjnego_vHMC_dla_XEN>.tar.gz` znajduje się plik **vhmc.cfg**. Otwórz plik **vhmc.cfg** w edytorze tekstu i zmodyfikuj następujące wartości:

- a. Zmień nazwę wirtualnej konsoli HMC (opcjonalne): sprawdź w pliku **vhmc.cfg** poprawność ścieżki do dysków. Plik zawiera łańcuch **DISK_PATH**.
- b. Zastąp wartość **DISK_PATH** ścieżką do pliku `disk1.img`:

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

c. Zastąp wartość **ethernet adapter** i dodaj adres MAC (opcjonalnie):

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

Opcjonalny adres MAC:

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

Uwaga: Po ponownym uruchomieniu wirtualnej konsoli HMC hiperwizor Xen automatycznie ponownie generuje adres MAC. Dodanie opcjonalnego adresu MAC rozwiąże ten problem.

d. Zastąp wartość **FLOPPYPATH** (jeśli jest używany mechanizm aktywacji):

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

7. Aby utworzyć i uruchomić maszynę wirtualną, uruchom następującą komendę: `xl create vHMC.cfg`.
8. Aby sprawdzić, czy maszyna wirtualna została dodana do listy zdefiniowanych maszyn wirtualnych, uruchom następującą komendę: `xl list`.
9. Aby uzyskać dostęp do lokalnej konsoli maszyny wirtualnej, wykonaj następującą komendę: `vncviewer localhost 0`.

Instalowanie wirtualnego urządzenia konsoli HMC przy użyciu oprogramowania VMware ESXi

Sekcja zawiera informacje na temat instalowania wirtualnego urządzenia konsoli Hardware Management Console (HMC) w środowisku VMware ESXi.

Wirtualne urządzenie konsoli HMC można zainstalować w środowisku VMware ESXi poprzez wdrożenie szablonu OVF (Open Virtualization Format) przy użyciu graficznego interfejsu użytkownika klienta vSphere.

Uwaga: Oprogramowanie VMware ESXi, na którym można zainstalować wirtualne urządzenie konsoli HMC, musi być w wersji 6.0 lub nowszej.

Aby zainstalować wirtualne urządzenie konsoli HMC w środowisku VMware ESXi przy użyciu klienta vSphere, wykonaj następujące kroki:

Uwaga: Składnia komendy może się różnić w zależności od systemu operacyjnego.

1. Pozyskaj plik archiwum TAR: <nazwa_pliku_instalacyjnego_vHMC_dla_VMware>.tgz.
2. Wyodrębnij plik OVA z archiwum TAR przy użyciu komendy `tar`.
3. Uruchom klienta vSphere i zaloguj się do hosta ESXi.
4. Wybierz w menu **File** (Plik) opcję **Deploy OVF template** (Wdróż szablon OVF).
5. Kliknij przycisk **Browse** (Przeglądaj) i wybierz plik OVA.
6. Kliknij przycisk **Next** (Dalej).
7. Po zakończeniu wdrożenia kliknij przycisk **Close** (Zamknij) i wybierz ikonę wirtualnego urządzenia konsoli HMC, aby włączyć wirtualne urządzenie konsoli HMC.

Instalowanie wirtualnego urządzenia konsoli HMC na serwerach POWER

Sekcja zawiera informacje na temat sposobu instalowania wirtualnego urządzenia konsoli Hardware Management Console (HMC) w zvirtualizowanym środowisku POWER.

Instalowanie wirtualnego urządzenia konsoli HMC w środowisku PowerVM (na partycji logicznej)

Sekcja zawiera informacje na temat sposobu instalowania wirtualnego urządzenia konsoli Hardware Management Console (HMC) w środowisku PowerVM.

Wirtualne urządzenie konsoli HMC obsługuje serwery z procesorem POWER9 i oprogramowaniem wbudowanym w wersji FW910 lub nowszej. Więcej informacji na ten temat zawiera strona [Supported](#)

Uwagi:

1. Nie można zarządzać serwerem, który udostępnia wirtualne urządzenie konsoli HMC.
2. Nie można zarządzać serwerem udostępniającym inne wirtualne urządzenie konsoli HMC, które zarządza serwerem udostępniającym bieżące wirtualne urządzenie konsoli HMC.

Na przykład założmy, że wirtualne urządzenie konsoli HMC A pracuje na serwerze A, a wirtualne urządzenie konsoli HMC B pracuje na serwerze B. wirtualne urządzenie konsoli HMC A nie może zarządzać serwerem B, gdy jednocześnie wirtualne urządzenie konsoli HMC B zarządza serwerem A. Jedno z wirtualnych urządzeń konsoli HMC może zarządzać drugim serwerem, ale oba wirtualne urządzenia konsoli HMC nie mogą wzajemnie zarządzać swoimi systemami w tym samym czasie.

Tworzenie zautomatyzowanego obrazu instalacyjnego konsoli HMC (opcjonalnie)

Możliwe jest utworzenie zautomatyzowanego obrazu instalacyjnego konsoli HMC, który pozwala na automatyczne zainstalowanie wirtualnego urządzenia konsoli HMC bez konieczności interakcji z kreatorem **HMC Installation** (Instalowanie konsoli HMC).

Uwaga: Wirtualne urządzenie konsoli HMC w środowisku PowerVM nie udostępnia obsługi adaptera graficznego dla adapterów przypisanych do partycji. Do nawiązania połączenia z konsolą HMC i obsługi interfejsu użytkownika można użyć obsługiwanej przeglądarki WWW.

Aby utworzyć zautomatyzowany obraz instalacyjny konsoli HMC, wykonaj następujące kroki:

1. Utwórz dwa katalogi, uruchamiając następujące komendy: `mkdir -p oldiso` i `mkdir -p newiso`.
2. Podłącz obraz instalacyjny konsoli HMC do katalogu **oldiso**, uruchamiając następującą komendę: `sudo mount -o loop <ścieżka_do_obrazu> oldiso`.
3. Skopiuj zawartość katalogu **oldiso** do katalogu **newiso**, uruchamiając następującą komendę: `cp -r oldiso/* newiso`.
4. Zmodyfikuj plik Grub dla instalacji zautomatyzowanej, uruchamiając następującą komendę: `sed -i 's/biosdevname=0/biosdevname=0 mode=auto optype=Install/' newiso/boot/grub/grub.cfg`.
5. Ustaw plik Grub jako tylko do odczytu, uruchamiając następującą komendę: `sudo chown 0444 newiso/boot/grub/grub.cfg`.
6. Utwórz nowy obraz instalacyjny ISO konsoli HMC, uruchamiając następującą komendę: `mkisofs -o <nazwa_nowego_obrazu_ISO> -V <etykieta_ISO> -f -r -T -udf --allow-limited-size --netatalk -chrp-boot -iso-level 4 -part -no-desktop -quiet newiso` (gdzie **etykieta ISO** musi mieć wartość HMC-<numer wersji i wydania konsoli HMC>, na przykład HMC-8.0.870.0).

Uwaga: Więcej informacji na temat konfigurowania mechanizmu aktywacji i pliku konfiguracyjnego zawiera sekcja [“Korzystanie z mechanizmu aktywacji w odniesieniu do wirtualnego urządzenia konsoli HMC”](#) na stronie 33.

Konfigurowanie woluminu logicznego

Aby skonfigurować wolumin logiczny, wykonaj następujące kroki:

1. Wybierz system zarządzany.
2. W menu kontekstowym wybierz kolejno opcje **System Actions** > **Power VM** > **Virtual Storage** (Działania systemowe > Power VM > Wirtualna pamięć masowa).
3. Wybierz kolejno opcje **Manage System VIOS** > **Action** > **Manage Virtual Storage** (Zarządzanie serwerem VIOS systemu > Działania > Zarządzanie wirtualną pamięcią masową).
4. Kliknij kartę **Virtual Disks** (Dyski wirtualne).

5. Kliknij opcję **Create virtual disk** (Utwórz dysk wirtualny) i wprowadź następujące informacje:

- **Virtual disk name** (Nazwa dysku wirtualnego): nazwa dysku wirtualnego.
- **Storage pool name** (Nazwa puli pamięci masowej): nazwa puli pamięci masowej.
- **Virtual disk size** (Wielkość dysku wirtualnego): wielkość dysku wirtualnego.
- **Assigned partition** (Przypisana partycja): nazwa partycji logicznej.

Uwaga: Wymagane jest minimum 160 GB miejsca na dysku (zalecane: 500 GB miejsca na dysku).

Konfigurowanie nośników instalacyjnych – tworzenie biblioteki nośników

Aby utworzyć bibliotekę nośników, wykonaj następujące kroki:

1. Wybierz system zarządzany.
2. W menu kontekstowym wybierz kolejno opcje **System Actions > Power VM > Virtual Storage** (Działania systemowe > Power VM > Wirtualna pamięć masowa).
3. Wybierz kolejno opcje **Manage System VIOS > Action > Manage Virtual Storage** (Zarządzanie serwerem VIOS systemu > Działania > Zarządzanie wirtualną pamięcią masową).
4. Kliknij kartę **Optical Devices** (Urządzenia optyczne).
5. Kliknij opcję **Create Library** (Utwórz bibliotekę) i wprowadź następujące informacje:
 - **Storage pool** (Pula pamięci masowej): nazwa puli pamięci masowej.
 - **Media library size** (Wielkość biblioteki nośników): wielkość biblioteki nośników.
6. Kliknij przycisk **OK**.

Konfigurowanie nośników instalacyjnych – przesyłanie nośników na serwer VIOS

Aby przesłać nośniki na wirtualny serwer we/wy (VIOS), wykonaj następujące kroki:

1. Zaloguj się do serwera VIOS.
2. W trybie użytkownika root serwera VIOS uruchom następującą komendę: `oem_setup_env`.
3. Aby zezwolić na połączenie z systemem NFS, uruchom następującą komendę: `nfs -o nfs_use_reserved_ports=1`.
4. Aby podłączyć system NFS do lokalnego folderu VIOS, uruchom następującą komendę: `mount <adres_IP_serwera>:/Mountpoint <folder_lokalny>`.
5. Aby sprawdzić, czy podłączony system NFS zawiera obraz instalacyjny ISO konsoli HMC i obraz konfiguracji mechanizmu aktywacji (opcjonalnie), uruchom następującą komendę: `ls`.

Konfigurowanie nośników instalacyjnych – łączenie nośników z biblioteką nośników

Aby połączyć nośniki z biblioteką nośników, wykonaj następujące kroki:

1. Przejdź z powrotem do opcji **Manage System VIOS > Action > Manage Virtual Storage** (Zarządzanie serwerem VIOS systemu > Działania > Zarządzanie wirtualną pamięcią masową) i kliknij kartę **Optical Devices** (Urządzenia optyczne).
2. W sekcji **Virtual Optical Media** (Wirtualne nośniki optyczne) wybierz opcję **Add Media** (Dodaj nośnik) z menu **Actions** (Działania).
3. W oknie **Add Virtual Media** (Dodawanie nośnika wirtualnego) wybierz opcję **Add existing file from VIOS filesystem** (Dodaj istniejący plik z systemu plików serwera VIOS) i wprowadź następujące informacje:
 - **Media name** (Nazwa nośnika): nazwa nośnika (na przykład HMCInstall lub AEDrive).
 - **Optical media file name** (Nazwa pliku nośnika optycznego): nazwa pliku instalacyjnego ISO (na przykład 01234567-ppc64ie.iso).
4. Kliknij przycisk **OK**.

5. Jeśli został utworzony obraz konfiguracji mechanizmu aktywacji, powtórz kroki od 3 do 4, aby dodać obraz konfiguracji mechanizmu aktywacji. W przeciwnym razie przejdź do kroku 6.
6. Sprawdź, czy nośnik optyczny został przesłany do biblioteki nośników, upewniając się, że nazwa nośnika jest wyświetlana na dostępnej liście **Virtual Optical Media** (Wirtualne nośniki optyczne).

Konfigurowanie partycji logicznej

Aby skonfigurować partycję logiczną, wykonaj następujące kroki:

1. Wybierz system zarządzany.
2. W menu kontekstowym wybierz kolejno opcje **System Actions** > **Partitions** > **Partitions** (Działania systemowe > Partycje > Partycje).
3. Kliknij opcję **Create Partition** (Utwórz partycję) i wprowadź następujące informacje:
 - **Partition Name** (Nazwa partycji): nazwa partycji.
 - **Partition ID** (ID partycji): identyfikator partycji.
 - **Partition Type** (Typ partycji): wybierz system operacyjny (**AIX/Linux** lub **IBM i**).
4. Kliknij przycisk **OK**.
5. Przydziel do partycji odpowiednią liczbę procesorów i ilość pamięci.
Uwaga: Wymagane są co najmniej 4 procesory i 8 GB pamięci.
6. W menu kontekstowym wybierz kolejno opcje **Partition Actions** > **Virtual I/O** > **Virtual Networks** (Działania na partycji > Wirtualne urządzenia we/wy > Sieci wirtualne).
7. Kliknij opcję **Attach Virtual Network** (Podłącz sieć wirtualną) i zaznacz pole wyboru **Show and attach new virtual ethernet adapters** (Pokaż i podłącz nowe adaptory wirtualnej sieci Ethernet). Wybierz w tabeli adaptory sieci wirtualnej, które mają zostać podłączone do partycji logicznej.
Uwaga: Dozwolone są maksymalnie cztery adaptory sieci wirtualnych.
8. W menu kontekstowym wybierz kolejno opcje **Partition Actions** > **Virtual I/O** > **Virtual Storage** (Działania na partycji > Wirtualne urządzenia we/wy > Wirtualna pamięć masowa).
9. Na karcie **Virtual Optical Device** (Wirtualne urządzenie optyczne) kliknij opcję **Add Virtual Optical Device** (Dodaj wirtualne urządzenie optyczne).
10. Wprowadź wartość w polu **Device Name** (Nazwa urządzenia), na przykład HMCInstall lub AEDrive, i wybierz z tabeli żądany serwer VIOS.
Uwaga: Zainstalowanie urządzenia AEDrive jest opcjonalne.
11. Kliknij przycisk **OK**.
12. Sprawdź, czy wirtualne urządzenia optyczne, które zostały dodane w kroku 10, znajdują się teraz w tabeli.
13. W menu **Action** (Działania) kliknij opcję **Load** (Załaduj).
14. Wybierz plik nośnika, który ma zostać przypisany do partycji logicznej, a następnie kliknij przycisk **OK**.
15. Sprawdź, czy wirtualne urządzenia optyczne załadowane w kroku 13 znajdują się teraz w tabeli.

Uruchamianie wirtualnego urządzenia konsoli HMC

Uwaga: W przypadku instalowania wirtualnego urządzenia konsoli HMC na partycji za pomocą pliku obrazu ISO konsoli HMC dostęp do interfejsu WWW z lokalnej konsoli graficznej nie jest możliwy.

Aby uruchomić wirtualne urządzenie konsoli HMC w środowisku PowerVM, wykonaj następujące kroki:

1. Wybierz partycję zarządzaną.
2. Otwórz aktywne połączenie z partycją logiczną, wybierając kolejno opcje **Actions** > **Console** > **Open Terminal Window** (Działania > Konsola > Otwórz okno terminala).
3. Aktywuj partycję logiczną, wybierając kolejno opcje **Actions** > **Activate** (Działania > Aktywuj).

4. Wybierz opcję **Activate (Normal)** (Aktywuj (Normalnie) i **Current Configuration** (Bieżąca konfiguracja).
5. Kliknij przycisk **Finish** (Zakończ).
6. Przejdź do okna terminala.
7. W menu **Boot** (Start) wybierz opcję **1 = SMS Menu** (1 = Menu SMS).
8. W menu głównym (**Main**) wybierz opcję **5 = Select Boot Options** (5 = Wybierz opcje startowe).
9. W menu **Multiboot** (Start wielu systemów) wybierz opcję **1 = Select Install/Boot Device** (1 = Wybór urządzenia instalacyjnego/startowego).
10. W menu **Select Device Type** (Wybór typu urządzenia) wybierz opcję **5 = List all devices** (5 = Pokaż wszystkie urządzenia).
11. Wybierz urządzenie HMCInstall na podstawie położenia urządzenia.
12. Wybierz opcję **2. Normal Mode Boot** (2. Start w trybie normalnym).
13. Wybierz opcję **1. Yes** (Tak), aby potwierdzić.
14. Postępuj zgodnie z instrukcjami wyświetlanymi na ekranie w kreatorze **HMC Install** (Instalowanie konsoli HMC).

Uwaga: Pomiń ten krok, jeśli jest używany zautomatyzowany obraz instalacyjny konsoli HMC.

15. Po zakończeniu instalacji i uruchomieniu systemu musisz wybrać język w oknie dialogowym **wyboru języka**.
16. Zaakceptuj umowę licencyjną.

Uwaga: Przed uruchomieniem jakiejkolwiek komendy upewnij się, że kontroler komendy jest gotowy do akceptowania komend. Na przykład uruchom komendę **lshmc -V** i zaczekaj na jej pomyślne zakończenie.

17. Zaloguj się jako użytkownik **hscroot** i skonfiguruj ustawienia sieciowe za pomocą komendy **chhmc**.

W poniższym przykładzie podano sekwencję komend **chhmc**, za pomocą których można skonfigurować sieć oraz włączyć w konsoli HMC protokół SSH (Secure Shell) i zdalny dostęp przez sieć WWW.

```
chhmc -c network -s modify -i ethX -a <adres IP konsoli HMC> -nm <maska sieci konsoli HMC>
      --lparcomm on
chhmc -c network -s modify -h <host konsoli HMC> -d <nazwa domeny konsoli HMC> -g <adres IP bramy>
chhmc -c network -s add -ns <serwer nazw> -ds <wyszukiwanie w domenach>
chhmc -c ssh -s enable
chhmc -c ssh.name -s add -a <adres IP>
chhmc -c SecureRemoteAccess.name -s add -a <adres IP>
chhmc -c remotewebui -s enable -i ethX
hmcshutdown -r -t now
```

- **ethX** to nazwa interfejsu sieciowego, który ma zostać skonfigurowany.
- **adres IP konsoli HMC** to adres IP konsoli HMC użytkownika.
- **maska sieci konsoli HMC** to maska sieci konsoli HMC użytkownika.
- **host konsoli HMC** to nazwa hosta konsoli HMC użytkownika.
- **nazwa domeny konsoli HMC** to nazwa domeny konsoli HMC użytkownika.
- **adres IP bramy** to adres IP bramy w sieci użytkownika.
- **serwer nazw** to adres serwera nazw sieci użytkownika.
- **wyszukiwanie w domenach** to nazwy domen, w których ma wyszukiwać konsola HMC.
- Aby umożliwić dostęp do wszystkich adresów IP, użyj opcji **-a 0.0.0.0 -nm 0** zamiast adresu IP.

Uwaga: W przypadku używania wielu adapterów wirtualnej sieci Ethernet należy dla każdego interfejsu uruchomić komendę **cat /etc/sysconfig/network-scripts/ifcfg-ethX** w wirtualnym urządzeniu konsoli HMC. Należy porównać adres MAC z adresem wyświetlanym przez konsolę HMC w widoku adaptera sieci wirtualnej partycji. Można kliknąć opcję **View Virtual Ethernet**

Adapter Settings (Wyświetl ustawienia adaptera wirtualnej sieci Ethernet), aby uzyskać informacje na temat adapterów wirtualnych sieci Ethernet. Ten krok pomoże określić poprawny interfejs do użycia.

18. Zrestartuj system.

Korzystanie z mechanizmu aktywacji w odniesieniu do wirtualnego urządzenia konsoli HMC

Sekcja zawiera informacje na temat sposobu korzystania z mechanizmu aktywacji w odniesieniu do wirtualnego urządzenia konsoli Hardware Management Console (HMC).

Mechanizm aktywacji jest strukturą, która umożliwia konfigurowanie poszczególnych komponentów maszyny wirtualnej podczas uruchamiania systemu. Aby skorzystać z mechanizmu aktywacji, należy utworzyć profil konfiguracji w postaci pliku XML, który umożliwi ustawienie wirtualnego urządzenia konsoli HMC w stan gotowości do zarządzania od pierwszego uruchomienia. Więcej informacji na temat konfigurowania pliku XML profilu konfiguracji zawiera sekcja [“Ustawienia profilu konfiguracji mechanizmu aktywacji” na stronie 33](#). W pliku konfiguracyjnym można konfigurować następujące opcje:

- ustawienie domyślnego układu klawiatury (Stany Zjednoczone),
- domyślne ustawienia narodowe (Stany Zjednoczone),
- wyłączenie konfigurowania klawiatury,
- wyłączenie konfigurowania ekranu,
- Umowa Licencyjna i Umowa na Kod Maszynowy,
- wyłączenie kreatora konfiguracji,
- wyłączenie kreatora zgłoszeń automatycznych,
- konfigurowanie maksymalnie czterech kart sieciowych,
- konfigurowanie ustawień firewalla dla każdego interfejsu,
- konfigurowanie interfejsu sieciowego jako serwera DHCP IPv4,
- konfigurowanie interfejsu prywatnego i otwartego,
- konfigurowanie urządzenia interfejsu bramy domyślnej.

Uwaga: Liczba adapterów Ethernet zdefiniowana w pliku konfiguracyjnym **vHMC-Conf.xml** musi być skorelowana z adapterami sieciowymi zdefiniowanymi w pliku konfiguracyjnym **domain.xml**, **vHMC.cfg** lub **VMWare**.

Mechanizm aktywacji wymaga dysku wirtualnego, który zawiera konfigurację XML. Plik **user_data** można edytować za pomocą edytora tekstu. Można przy tym użyć wskazówek dotyczących konfigurowania XML przedstawionych w poniższym przykładzie.

Aby utworzyć obraz dysku wirtualnego w standardzie ISO z konfiguracją mechanizmu aktywacji w środowisku Linux, wykonaj następujące kroki:

1. Utwórz katalog:

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

2. Skopiuj zmodyfikowany plik **user_data** do katalogu:

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

3. Utwórz obraz dysku wirtualnego z konfiguracją mechanizmu aktywacji:

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

Ustawienia profilu konfiguracji mechanizmu aktywacji

Sekcja zawiera ustawienia pliku konfiguracyjnego mechanizmu aktywacji wprowadzane za pomocą znaczników XML.

Plik konfiguracyjny

Korzystając z następującego przykładowego pliku konfiguracyjnego, można uzyskać informacje na temat znaczników 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>
```

Znaczniki XML w pliku konfiguracyjnym

Za pomocą znaczników XML można w pliku konfiguracyjnym mechanizmu aktywacji ustawić konkretne wartości poszczególnych atrybutów. Wartości te można ręcznie ustawiać w pliku konfiguracyjnym mechanizmu aktywacji. W następującej tabeli opisano poszczególne znaczniki i ich dozwolone wartości:

Tabela 9. Znaczniki XML			
Znaczniki	Opis	Dopuszczalne wartości	Uwagi
ConfigurationVersion	Element wymagany definiujący wersję konfiguracji, która ma zostać użyta.	2.0	
LicenseAgreement	Element wymagany służący do wyświetlenia umowy licencyjnej wirtualnego urządzenia konsoli HMC.		

Tabela 9. Znaczniki XML (kontynuacja)			
Znaczniki	Opis	Dopuszczalne wartości	Uwagi
AcceptLicense	Element wymagany służący do zaakceptowania umowy licencyjnej wirtualnego urządzenia konsoli HMC.	Yes: akceptacja umowy licencyjnej konsoli HMC. No: prośba o zaakceptowanie umowy licencyjnej konsoli HMC przez użytkownika.	Jeśli wprowadzono niepoprawną wartość, mechanizm aktywacji użyje domyślnego ustawienia No .
Locale	Element wymagany, który służy do zdefiniowania ustawień narodowych.	en_US.UTF-8	Jeśli wprowadzono niepoprawną wartość, mechanizm aktywacji użyje domyślnego ustawienia US .
SetupWizard	Element wymagany, który służy do włączenia lub wyłączenia kreatora konfiguracji konsoli HMC (HMC Setup).	Yes: kreator HMC Setup (Konfiguracja konsoli HMC) będzie wyświetlany. No: wyświetlanie kreatora HMC Setup (Konfiguracja konsoli HMC) jest wyłączone.	Jeśli wprowadzono niepoprawną wartość, mechanizm aktywacji użyje domyślnego ustawienia Yes .
SetupCallHomeWizard	Element wymagany, który służy do włączenia lub wyłączenia kreatora zgłoszeń automatycznych (HMC Call).	Yes: kreator HMC Call Home (Zgłoszenia automatyczne konsoli HMC) będzie wyświetlany. No: wyświetlanie kreatora HMC Call Home (Zgłoszenia automatyczne konsoli HMC) jest wyłączone.	Jeśli wprowadzono niepoprawną wartość, mechanizm aktywacji użyje domyślnego ustawienia Yes .
SetupKeyboard	Element wymagany służący do zdefiniowania konfiguracji klawiatury.	Yes: będzie wyświetlane pytanie o konfigurację klawiatury. No: akceptowana jest domyślna konfiguracja klawiatury (US).	Jeśli wprowadzono niepoprawną wartość, mechanizm aktywacji użyje domyślnego ustawienia Yes .
SetupDisplay	Element wymagany służący do włączenia lub wyłączenia konfiguracji terminala.	Yes: pytanie o konfigurację terminala będzie wyświetlane. No: akceptowana jest domyślna konfiguracja terminala.	Jeśli wprowadzono niepoprawną wartość, mechanizm aktywacji użyje domyślnego ustawienia Yes .

Tabela 9. Znaczniki XML (kontynuacja)

Znaczniki	Opis	Dopuszczalne wartości	Uwagi
Ethernet	Element wymagany, który zawiera wartości konfiguracji adaptera Ethernet. Można skonfigurować maksymalnie cztery adaptery Ethernet.	Enable: Yes: należy skonfigurować ten adapter. No: nie należy konfigurować tego adaptera. DefaultGatewayDevice: Yes: należy skonfigurować ten adapter jako główny adapter sieciowy. No: nie należy konfigurować tego adaptera jako głównego adaptera sieciowego. PrivateInterface: Yes: należy skonfigurować ten adapter jako interfejs prywatny. Opcję Yes należy wybrać w sytuacji, gdy interfejs ma zostać skonfigurowany jako serwer DHCP IPv4. No: nie należy konfigurować tego adaptera jako interfejsu prywatnego. Opcję No należy wybrać w sytuacji, gdy typ interfejsu ma zostać skonfigurowany jako statyczny IPv4.	Mechanizm aktywacji jest uruchamiany z konfiguracją domyślną, jeśli w sekcji adaptera Ethernet wprowadzono jakąkolwiek niepoprawną wartość lub zdefiniowano wiele domyślnych urządzeń bramy . Elementy opcjonalne można pominąć w konfiguracji. Wymagana jest co najmniej jedna konfiguracja protokołu IPV4 lub IPV6. Jeśli konfiguracja protokołu IP nie zostanie podana, mechanizm aktywacji użyje konfiguracji domyślnej.
HostName	Element opcjonalny służący do definiowania nazwy sieciowej hosta.	Dowolny poprawny łańcuch nazwy hosta.	Jeśli nie zdefiniowano żadnego elementu, mechanizm aktywacji użyje domyślnej wartości hosta lokalnego HostName .
Domain	Element opcjonalny służący do definiowania domeny sieciowej.	Dowolna poprawna wartość domeny (na przykład przyklad.com.pl).	Jeśli nie zdefiniowano tego elementu, mechanizm aktywacji użyje domyślnej wartości pustej Domain .

Tabela 9. Znaczniki XML (kontynuacja)

Znaczniki	Opis	Dopuszczalne wartości	Uwagi
DNSServers	Element opcjonalny służący do definiowania sieciowych serwerów DNS.	Dopuszczalne jest skonfigurowanie jednej wartości serwera DNS lub maksymalnie trzech poprawnych adresów IPv4 lub IPv6 rozdzielonych przecinkami. • Przykład 1: IPv4: 8.3.2.1 IPv6: 2001:4860:4860::8888 • Przykład 2: IPv4: 8.3.2.1,8.5.4.1 IPv6: 2001:4860:4860::8888,2001:4860:4860::8844 • Przykład 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	Jeśli nie zdefiniowano tego elementu, mechanizm aktywacji użyje domyślnej wartości pustej DNSServers .
IP4Config	Element opcjonalny służący do definiowania ustawień konfiguracyjnych protokołu IPv4.	IPType: element wymagany służący do definiowania typu konfiguracji protokołu IPv4. • Static: skonfigurowanie tego adaptera z użyciem konfiguracji statycznej. • DHCP: skonfigurowanie tego adaptera z użyciem konfiguracji protokołu DHCP. • DHCPServer: skonfigurowanie tego adaptera jako serwera DHCP IPv4 (wymaga ustawienia znacznika PrivateInterface na wartość Yes). IPAddress: element opcjonalny, który jest wymagany tylko wtedy, gdy wybrano konfigurację Static lub DHCPServer. • Static Configuration: dowolna poprawna wartość adresu IPv4. • DHCPServer Configuration: dowolny adres IP serwera DHCP mieszczący się w zakresie adresów IP. Netmask: element opcjonalny, który jest wymagany tylko wtedy, gdy wybrano konfigurację Static. • Dowolna poprawna wartość maski sieci IPv4. Gateway: element opcjonalny, który jest wymagany tylko wtedy, gdy wybrano konfigurację Static. • Dowolna poprawna wartość maski sieci IPv4.	

Tabela 9. Znaczniki XML (kontynuacja)

Znaczniki	Opis	Dopuszczalne wartości	Uwagi
IP6Config	Element opcjonalny służący do definiowania ustawień konfiguracyjnych protokołu IPv6.	IPTyp: element wymagany służący do zdefiniowania typu konfiguracji protokołu IPv6. • Static: skonfigurowanie tego adaptera z użyciem konfiguracji statycznej. • DHCP: skonfigurowanie tego adaptera z użyciem konfiguracji protokołu DHCP. IPAdres: może mieć formę długą lub krótką formatu IPv6 oraz formę długą lub krótką przedrostka IPv6. • Przykład 1: IPv6: 2001:4860:4860:0000:0000:0000:8888 • Przykład 2: IPv6: 2001:4860:4860::8888 • Przykład 3: IPv6: 2001:4860:4860::8888/128 Jeśli nie podano przedrostka, mechanizm aktywacji użyje domyślnego ustawienia prefiksu /64. Gateway: • Dowolna poprawna wartość adresu IPv6.	

Tabela 9. Znaczniki XML (kontynuacja)

Znaczniki	Opis	Dopuszczalne wartości	Uwagi
Firewall	Element opcjonalny służący do definiowania ustawień firewalla.	PEGASUS: • Enabled: zezwolenie na otwarcie portów PEGASUS. • Disabled: wyłączenie portów PEGASUS. RPD: • Enabled: zezwolenie na otwarcie portów RMC. • Disabled: wyłączenie portów RMC. FCS: • Enabled: zezwolenie na otwarcie portów FCS. • Disabled: wyłączenie portów FCS. I5250: • Enabled: zezwolenie na otwarcie portów 5250. • Disabled: wyłączenie porty 5250. PING: • Enabled: zezwolenie na otwarcie portu Ping. • Disabled: wyłączenie portu Ping. L2TP: • Enabled: zezwolenie na otwarcie portów L2TP. • Disabled: wyłączenie portów L2TP. SLP: • Enabled: zezwolenie na otwarcie portów SLP. • Disabled: wyłączenie portów SLP. RSCT: • Enabled: zezwolenie na otwarcie portów RSCT. • Disabled: wyłączenie portów RSCT. SECUREREMOTEACCESS: • Enabled: zezwolenie na otwarcie portów bezpiecznego zdalnego dostępu. • Disabled: wyłączenie portów bezpiecznego zdalnego dostępu. SSH: • Enabled: zezwolenie na otwarcie portu SSH. • Disabled: wyłączenie portu SSH.	

Tabela 9. Znaczniki XML (kontynuacja)			
Znaczniki	Opis	Dopuszczalne wartości	Uwagi
Firewall	Element opcjonalny służący do definiowania ustawień firewalla.	NTP: • Enabled: zezwolenie na otwarcie portów NTP. • Disabled: wyłączenie portów NTP. SNMPTraps: • Enabled: zezwolenie na otwarcie portów pułapek SNMP. • Disabled: wyłączenie portów pułapek SNMP. SNMPAgents: • Enabled: zezwolenie na otwarcie portów agentów SNMP. • Disabled: wyłączenie portów agentów SNMP.	
NTPServers	Znacznik NTPServers jest potrzebny, jeśli użytkownik chce skonfigurować nie więcej niż pięć serwerów NTP w ramach wirtualnego urządzenia konsoli HMC.	NTPServers: akceptuje wartości <ntpparam ntpserver="server" ntpversion="version"/> ntpparam: • ntpserver: akceptuje dowolne poprawne wartości IPv4 lub IPv6 i poprawne nazwy hosta. • ntpversion: akceptuje wartość liczbową 1-4 Przykład: <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>	

Konfigurowanie konsoli HMC

Sekcja zawiera informacje dotyczące konfigurowania połączeń sieciowych, konfigurowania konsoli HMC, wykonywania czynności po konfiguracji i aktualizowania konsoli HMC.

Wybór ustawień sieciowych konsoli HMC

Sekcja zawiera informacje na temat dostępnych ustawień sieciowych konsoli HMC.

Połączenia sieciowe konsoli HMC

Sekcja zawiera opis działania konsoli HMC w sieci.

Można użyć różnych typów połączeń sieciowych, aby połączyć konsolę HMC z systemem zarządzanym. Więcej informacji na temat konfigurowania konsoli HMC do połączenia z siecią zawiera sekcja [“Konfigurowanie konsoli HMC” na stronie 57](#). Więcej informacji na temat używania konsoli HMC w sieci zawierają następujące informacje.

Typy połączeń sieciowych konsoli HMC

Sekcja zawiera informacje na temat używania funkcji zdalnego zarządzania i serwisu konsoli HMC za pośrednictwem sieci.

Konsola HMC obsługuje następujące typy połączeń logicznych:

Połączenie konsoli HMC z systemem zarządzanym

Ten typ połączenia jest używany do wykonywania większości funkcji zarządzania sprzętem, w których żądania funkcji sterujących są przesyłane przez konsolę HMC za pośrednictwem procesora serwisowego systemu zarządzanego. Połączenie między konsolą HMC i procesorem serwisowym jest czasem nazywane *siecią serwisową*. Połączenie to jest niezbędne do zarządzania systemem zarządzanym.

Połączenie konsoli HMC z partycją logiczną

Ten typ połączenia jest używany do zbierania informacji związanych z platformą (na temat błędów sprzętu oraz zasobów sprzętowych) z systemów operacyjnych uruchomionych na partycjach logicznych, a także do koordynowania niektórych działań platformy (dynamicznego partycjonowania logicznego oraz napraw w trakcie pracy systemu) z działaniem tych systemów operacyjnych. Utworzenie tego połączenia jest konieczne, jeśli mają być używane funkcje powiadamiania o błędach i zdarzeniach serwisowych.

Połączenie konsoli HMC z kontrolerem BMC

Uwaga: Połączenie z kontrolerem BMC ma zastosowanie tylko do konsoli HMC model 7063-CR1.

Służy ono do wykonywania czynności serwisowych i konserwacyjnych. Połączenie z kontrolerem BMC umożliwia ładowanie i konserwację oprogramowania wbudowanego konsoli HMC w systemie. To połączenie jest wymagane do uzyskania dostępu do kontrolera BMC na konsoli HMC.

Połączenie konsoli HMC z użytkownikami zdalnymi

Ten typ połączenia umożliwia użytkownikom zdalnym dostęp do funkcji konsoli HMC. Użytkownicy zdalni mogą uzyskać dostęp do konsoli HMC na następujące sposoby:

- Poprzez użycie przeglądarki WWW do uzyskania zdalnego dostępu do wszystkich funkcji interfejsu GUI konsoli HMC.
- Poprzez użycie protokołu SSH do uzyskania zdalnego dostępu do funkcji wiersza komend konsoli HMC.
- Poprzez użycie serwera terminali wirtualnych do uzyskania zdalnego dostępu do wirtualnych konsol partycji logicznych.

Połączenie konsoli HMC z serwisem i wsparciem

Ten typ połączenia jest używany do przekazywania od i do dostawcy usług takich danych, jak raporty o błędach sprzętu, dane spisu zasobów oraz aktualizacje mikrokodu. Ta ścieżka komunikacyjna może być skonfigurowana w taki sposób, aby umożliwić wykonywanie automatycznych zgłoszeń serwisowych.

Konsola HMC obsługuje maksymalnie cztery fizycznie odrębne interfejsy Ethernet. W wersji autonomicznej konsola HMC obsługuje tylko trzy interfejsy, w tym jeden zintegrowany adapter Ethernet i nie więcej niż dwa adaptory dodatkowe. Każdy z tych interfejsów powinien być użyty w następujący sposób:

- Jeden interfejs sieciowy powinien być używany wyłącznie do komunikacji między konsolą HMC a systemem zarządzanym, co oznacza, że w tej sieci znajdowałyby się tylko konsola HMC i procesory serwisowe. Co najmniej jeden interfejs sieciowy powinien być używany wyłącznie do komunikacji między konsolą HMC a systemem zarządzanym, co oznacza, że w tej sieci znajdowałyby się tylko konsola HMC i procesory serwisowe systemów zarządzanych. Chociaż interfejsy sieciowe w procesorach serwisowych są szyfrowane za pomocą protokołu SSL i chronione hasłem, posiadanie osobnej, dedykowanej sieci zapewnia wyższy poziom bezpieczeństwa dla tych interfejsów.
- Interfejs sieci otwartej jest zwykle używany dla połączenia sieciowego między konsolą HMC a partycjami logicznymi w systemach zarządzanych, do komunikacji między konsolą HMC a partycjami logicznymi. Interfejsu sieci otwartej można też użyć do zdalnego zarządzania konsolą HMC.

- Opcjonalnie można użyć trzeciego interfejsu, aby połączyć się z partycjami logicznymi i zarządzać zdalnie konsolą HMC. Ten interfejs może być również używany do oddzielnego połączenia konsoli HMC z różnymi grupami partycji logicznych. Może na przykład zaistnieć potrzeba wykorzystania administracyjnej sieci LAN oddzielnej od sieci LAN służącej do przeprowadzania większości zwykłych transakcji. Za pomocą tej metody zdalni administratorzy mogą uzyskać dostęp do konsoli HMC oraz innych jednostek zarządzanych. Czasem partycje logiczne należą do różnych domen bezpieczeństwa sieciowego, a czasem są chronione przez firewall, może zatem zaistnieć potrzeba utworzenia różnych połączeń sieciowych konsoli HMC z każdą z tych domen.

Konsola HMC – wymagania dotyczące przeglądarek WWW

Konsola HMC w wersji 9.1.0 jest obsługiwana przez przeglądarki Google Chrome w wersji 57, Microsoft Internet Explorer (IE) w wersji 11.0, Mozilla Firefox w wersjach 45 i 52 Extended Support Release (ESR) oraz Safari w wersji 10.1.

Jeśli przeglądarka jest skonfigurowana w taki sposób, aby korzystała z internetowego serwera proxy, do listy wyjątków należy dodać lokalne adresy internetowe. Aby uzyskać więcej informacji na temat listy wyjątków, skontaktuj się z administratorem sieci. Jeśli uzyskanie dostępu do konsoli HMC wymaga korzystania z serwera proxy, należy kliknąć kolejno opcje Narzędzia > Opcje internetowe > Zaawansowane i zaznaczyć opcję Użyj protokołu HTTP 1.1 dla połączeń przez serwer proxy.

Obsługa informacji cookie sesji musi być włączona, aby interfejs ASMI mógł działać podczas zdalnego połączenia z konsolą HMC. Kod proxy interfejsu zapisuje informacje o sesji i korzysta z nich. Aby włączyć obsługę informacji cookie dotyczących sesji, wykonaj następujące czynności.

Włączanie informacji cookie dotyczących sesji w przeglądarce Internet Explorer.

1. Kliknij menu Narzędzia, a następnie kliknij element Opcje internetowe.
2. Kliknij kartę Prywatność, a następnie kliknij przycisk Zaawansowane.
3. Upewnij się, że zaznaczona jest opcja Zawsze zezwalaj na pliki cookie dotyczące sesji. Jeśli opcja ta nie jest zaznaczona, wybierz opcję Zastąp automatyczną obsługę plików cookie, a następnie wybierz opcję Zawsze zezwalaj na pliki cookie dotyczące sesji.
4. Zaznacz opcje Monitoruj w kolumnach Pliki cookie tej samej firmy i Pliki cookie innych firm.
5. Kliknij przycisk OK.

Włączanie informacji cookie dotyczących sesji w przeglądarce Firefox.

1. Kliknij menu Narzędzia, a następnie kliknij element Opcje.
2. Kliknij kartę Ciasteczka.
3. Zaznacz opcję Zezwólaj witrynom na ustawianie ciasteczek.
4. Zaznacz opcję Wyjątki i dodaj konsolę HMC.
5. Kliknij przycisk OK.

Sieci prywatne i otwarte w środowisku konsoli HMC

Konsola HMC może zostać skonfigurowana do pracy w sieciach otwartych i prywatnych. Sieci prywatne umożliwiają korzystanie z wybranego zakresu nieroutowalnych adresów IP. Sieć *publiczna*, czyli "otwarta", oznacza połączenie sieciowe między konsolą HMC a wszelkimi partycjami logicznymi i innymi systemami w zwykłej sieci lokalnej.

Sieci prywatne

Jedynymi urządzeniami w sieci prywatnej konsoli HMC są sama konsola i systemy zarządzane, do których jest ona podłączona. Konsola HMC jest podłączona do procesora serwisowego FSP (Flexible Service Processor) każdego systemu zarządzanego.

W większości systemów procesor FSP udostępnia dwa porty Ethernet oznaczone jako **HMC1** i **HMC2**. Można podłączyć maksymalnie dwie konsole HMC.

Niektóre systemy są wyposażone w opcję podwójnego procesora FSP. W takiej sytuacji drugi procesor FSP pełni funkcję nadmiarowego procesora zapasowego. Podstawowe wymagania konfiguracyjne systemu z dwoma procesorami FSP są generalnie takie same, jak w przypadku systemów bez drugiego procesora FSP. Konsola HMC musi być podłączona do każdego z procesorów FSP, w związku z czym obecność więcej niż jednego procesora FSP lub wielu systemów zarządzanych wymaga użycia większej ilości sprzętu sieciowego (na przykład przełącznika lub koncentratora sieci LAN).

Uwaga: Każdy port FSP w systemie zarządzanym może być podłączony tylko do jednej konsoli HMC.

Sieci publiczne

Sieć otwarta może być podłączona do firewalla lub routera w celu uzyskiwania dostępu do Internetu. Dostępność połączenia z Internetem pozwala konsoli HMC automatycznie nawiązywać połączenie z działem wsparcia w razie wystąpienia błędów sprzętowych wymagających zgłoszenia.

Konsola HMC ma własny firewall na każdym ze swoich interfejsów sieciowych. Podstawowa konfiguracja firewalla jest automatycznie tworzona po uruchomieniu na konsoli HMC Kreatora instalacji z przewodnikiem, ale po zakończeniu wstępnego instalowania i konfigurowania konsoli HMC można dostosować ustawienia firewalla do konkretnych potrzeb.

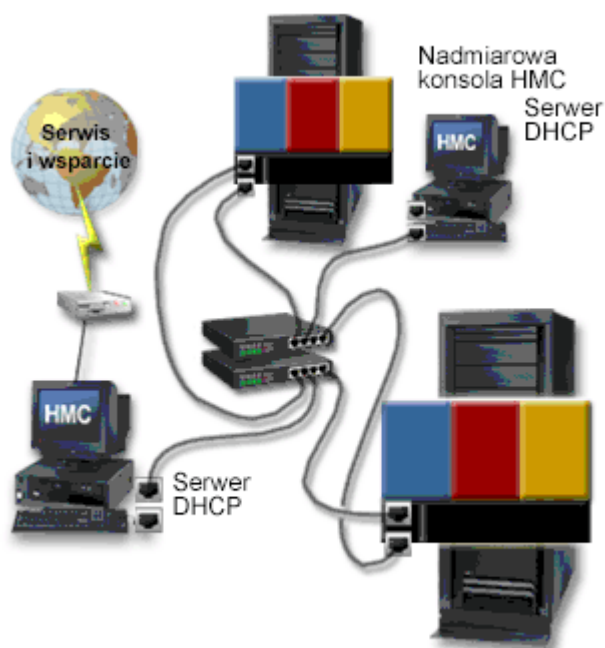
Konsola HMC jako serwer DHCP

Konsola HMC może pełnić funkcję serwera DHCP.

W przypadku skonfigurowania pierwszego interfejsu sieciowego jako sieci prywatnej do wyboru jest kilka zakresów adresów IP, które zostaną przypisane przez serwer DHCP poszczególnym klientom. Dostępne zakresy adresów zawierają segmenty standardowych nieroutowalnych zakresów adresów IP.

Poza tymi standardowymi zakresami istnieje również specjalny zakres adresów IP zarezerwowany dla adresów IP. Ten specjalny zakres pozwala uniknąć konfliktów, gdy sieci otwarte połączone z konsolą HMC używają jednego z nieroutowalnych zakresów adresów. Na podstawie wybranego zakresu do interfejsu sieciowego konsoli HMC w sieci prywatnej zostanie automatycznie przypisany pierwszy adres IP z tego zakresu, a procesorom serwisowym zostaną przypisane pozostałe adresy zakresu.

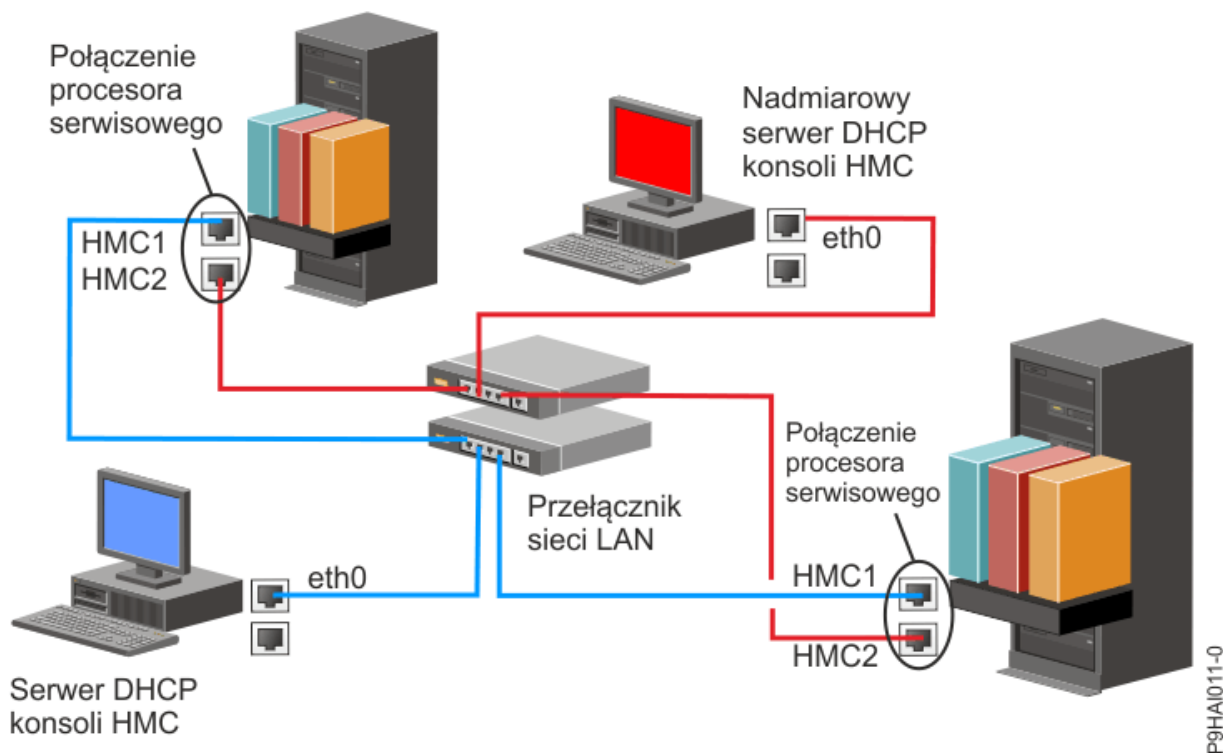
Serwer DHCP w konsoli HMC korzysta z automatycznego przydzielania, co oznacza, że każdy unikalny interfejs sieci Ethernet procesora serwisowego będzie miał ponownie przypisany ten sam adres IP przy każdym uruchomieniu. Każdy interfejs sieci Ethernet ma unikalny identyfikator oparty na wbudowanym adresie MAC (Media Access Control), co pozwala na ponowne przypisywanie przez serwer DHCP tych samych parametrów IP. Można skonfigurować oba porty konsoli HMC **eth0** i **eth1**, aby podawały adresy DHCP. Można skonfigurować oba porty konsoli HMC **eth0** i **eth1**, aby podawały adresy DHCP.



Rysunek 9. Sieć prywatna z jedną konsolą HMC pełniącą funkcje serwera DHCP

Uwaga: Jeśli wykorzystywany jest protokół IPv6, proces wykrywania musi być wykonany ręcznie. W przypadku protokołu IPv6 automatyczne wykrywanie nie jest dostępne.

Więcej informacji na temat konfigurowania konsoli HMC jako serwera DHCP zawiera sekcja “Konfigurowanie konsoli HMC jako serwera DHCP” na stronie 66.



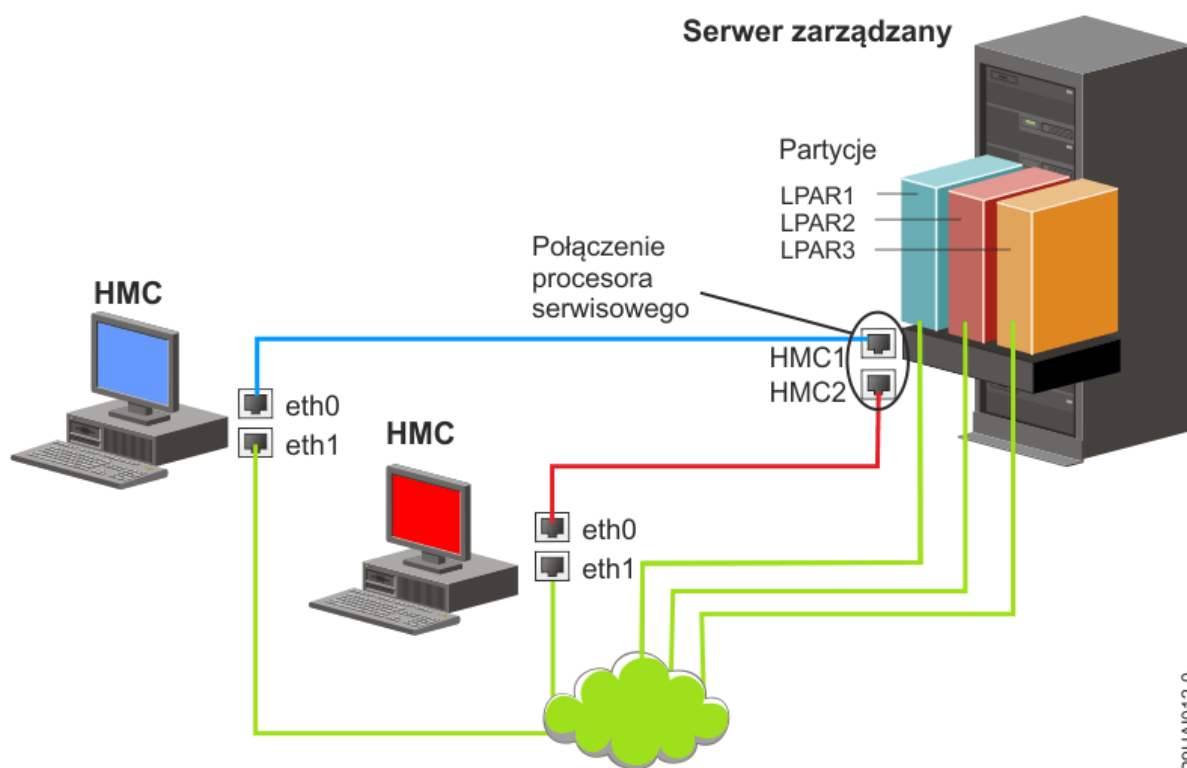
Na rysunku przedstawiono nadmiarowe środowisko konsoli HMC z dwoma systemami zarządzanymi. Pierwsza konsola HMC jest podłączona do pierwszego portu każdego procesora FSP, a nadmiarowa konsola HMC jest podłączona do drugiego portu procesora FSP. Każda konsola HMC jest skonfigurowana jako serwer DHCP przy użyciu innego zakresu adresów IP. Połączenia znajdują się w osobnych sieciach

prywatnych. Z tego względu bardzo ważne jest, aby żaden port FSP nie był podłączony do więcej niż jednej konsoli HMC.

Port FSP każdego systemu zarządzanego, który jest podłączony do konsoli HMC, wymaga niepowtarzalnego adresu IP. W celu zapewnienia niepowtarzalności adresu IP każdego procesora FSP należy używać wbudowanej w konsolę HMC funkcji serwera DHCP. W chwili wykrycia przez procesor FSP aktywnego łącza sieciowego wysyłane jest żądanie rozgłoszeniowe w celu zlokalizowania serwera DHCP. Poprawnie skonfigurowana konsola HMC odpowiada na takie żądanie poprzez przydzielenie adresu z określonego zakresu.

Jeśli używanych jest wiele procesorów FSP, do połączenia konsoli HMC z prywatną siecią procesorów FSP konieczny jest przełącznik lub koncentrator sieci LAN. Inną możliwością jest wydzielenie tego segmentu sieci jako prywatnej *wirtualnej sieci LAN* (VLAN), obejmującej kilka portów na większym przełączniku zarządzanym. Jeśli używanych jest wiele prywatnych sieci VLAN, należy się upewnić, że są one odizolowane i bez krzyżowego ruchu sieciowego.

Jeśli w danym środowisku używanych jest kilka konsol HMC, należy każdą z nich podłączyć do partycji logicznych i pozostałych konsol HMC w tej samej sieci otwartej.



Na rysunku przedstawiono dwie konsole HMC podłączone do pojedynczego serwera zarządzanego w sieci prywatnej oraz do trzech partycji logicznych w sieci publicznej. Do konsoli HMC można dodać jeszcze jeden adapter Ethernet, aby dysponowała ona trzema interfejsami sieciowymi. Tej trzeciej sieci można używać jako sieci zarządzania lub podłączyć ją do serwera zarządzającego CSM (Cluster Systems Manager).

Wybór metody połączenia dla serwera zgłoszeń automatycznych

Sekcja zawiera informacje na temat różnych możliwości połączenia z wykorzystaniem serwera zgłoszeń automatycznych.

Konsolę HMC można skonfigurować w taki sposób, aby możliwe było wysyłanie informacji dotyczących serwisowania sprzętu do IBM za pośrednictwem połączenia internetowego przez sieć LAN lub połączenia modemowego.

Komunikację za pośrednictwem połączenia internetowego opartego na sieci LAN można skonfigurować na dwa sposoby. Pierwszym sposobem jest wykorzystanie standardowego protokołu SSL (Secure Sockets

Layer). Możliwe jest wykorzystanie komunikacji z szyfrowaniem SSL do łączenia z Internetem za pośrednictwem serwera proxy. Komunikacja SSL będzie prawdopodobnie bardziej zgodna z wytycznymi firmy w zakresie bezpieczeństwa.

Uwaga: Jeśli używany interfejs do sieci otwartej korzysta wyłącznie z protokołu IP w wersji 6 (IPv6), nie będzie możliwe nawiązywanie połączenia internetowego z działem wsparcia przez sieć VPN. Więcej informacji na temat używanych protokołów zawiera sekcja [“Wybór protokołu internetowego”](#) na stronie 47.

Zalety korzystania z połączenia internetowego to między innymi:

- większa szybkość transmisji,
- obniżenie kosztów ponoszonych przez klienta (na przykład kosztu utrzymywania dedykowanej analogowej linii telefonicznej),
- większa niezawodność.

Następujące zabezpieczenia są stosowane zawsze, niezależnie od wybranej metody połączenia:

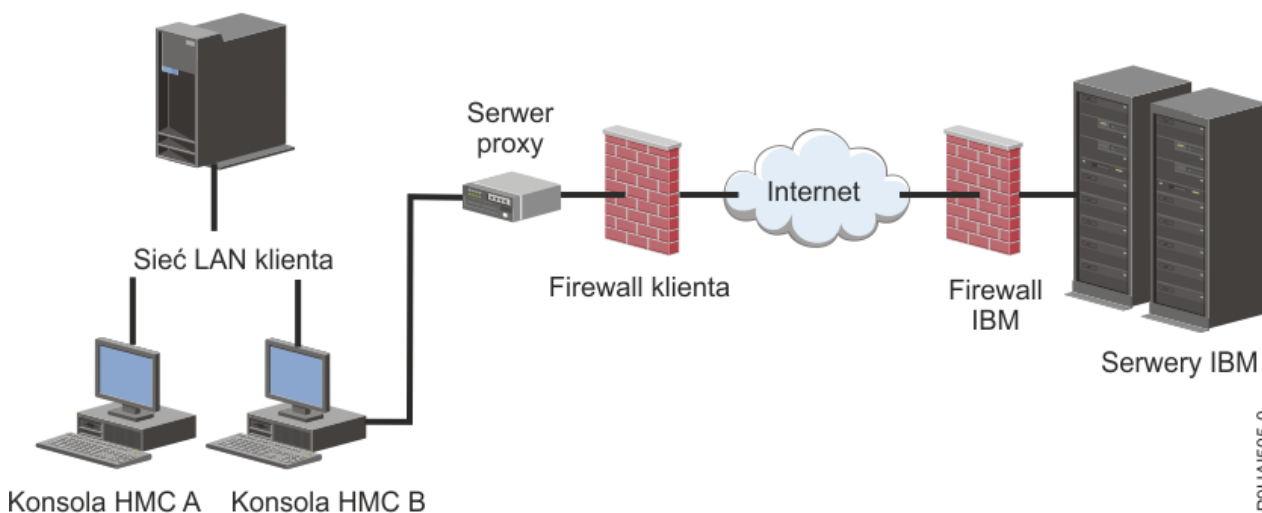
- Żądania zdalnego wsparcia są zawsze inicjowane przez konsolę HMC i przesyłane do IBM. System obsługi serwisowej IBM nigdy nie inicjuje połączenia przychodzącego.
- Wszystkie dane przesyłane między konsolą HMC a systemem obsługi serwisowej IBM są szyfrowane z użyciem silnych algorytmów kryptograficznych. W zależności od wybranej metody łączenia do szyfrowania używany jest protokół SSL lub IPsec ESP (Encapsulating Security Payload).
- Podczas nawiązywania połączenia szyfrowanego konsola HMC uwierzytelnia system docelowy jako system obsługi serwisowej IBM.

Dane przesyłane do systemu obsługi serwisowej IBM obejmują wyłącznie opisy problemów sprzętowych i konfiguracji. Do IBM nie są przesyłane żadne dane aplikacji ani dane klienta.

Korzystanie z pośredniego połączenia internetowego przy użyciu serwera proxy

Jeśli sposób zainstalowania konsoli HMC wymaga, aby pracowała ona w sieci prywatnej, to często możliwe jest pośrednie nawiązywanie połączenia z użyciem serwera proxy obsługującego SSL, który będzie przekazywać żądania do Internetu. Inną potencjalną zaletą korzystania z serwera proxy SSL jest to, że może on oferować funkcje rejestrowania w dzienniku i kontroli.

Aby było możliwe przekazywanie gniazd SSL, serwer proxy musi obsługiwać podstawowe funkcje nagłówków proxy (zgodnie ze specyfikacją RFC 2616) oraz metodę CONNECT. Opcjonalnie można też włączyć podstawowe uwierzytelnianie serwera proxy (RFC 2617), aby przed próbą przekazania gniazd za pośrednictwem serwera proxy następowało uwierzytelnienie konsoli HMC.

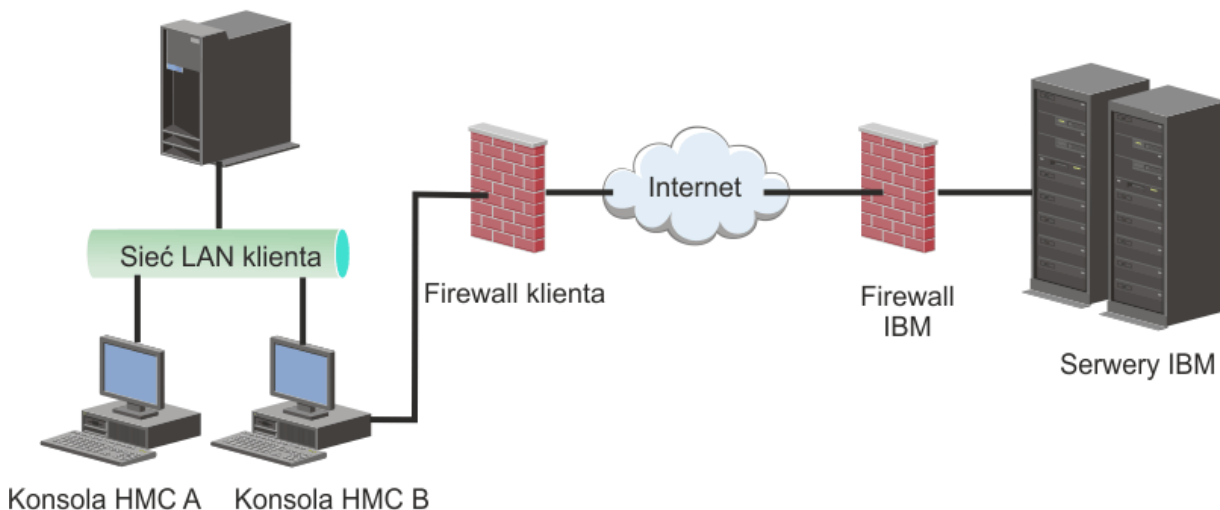


Aby była możliwa komunikacja z konsolą HMC, serwer proxy klienta musi dopuszczać połączenia na porcie 443. Serwer proxy można skonfigurować tak, aby ograniczał zakres adresów IP, z którymi może się

łączyć konsola HMC. Listę adresów IP zawiera sekcja [“Listy adresów do internetowych połączeń SSL”](#) na stronie 47.

Korzystanie z bezpośredniego połączenia internetowego SSL

Z bezpośredniego połączenia internetowego można korzystać wtedy, gdy możliwe jest podłączenie konsoli HMC do Internetu i takie skonfigurowanie zewnętrznego firewalla, aby przepuszczał on pakiety wychodzące dla połączeń TCP nawiązanych z adresami docelowymi wymienionymi w sekcji [“Listy adresów do internetowych połączeń SSL”](#) na stronie 47.



Łączenie się ze zdalnym wsparciem za pomocą internetowego połączenia SSL

Całość komunikacji odbywa się za pośrednictwem gniazd TCP zainicjowanych przez konsolę HMC, a do szyfrowania przesyłanych danych jest używane silne szyfrowanie SSL. Aby można było skonfigurować przepuszczanie takich połączeń przez zewnętrzne firewalle, publikowane są adresy docelowe TCP/IP (patrz [“Listy adresów do internetowych połączeń SSL”](#) na stronie 47).

Uwaga: Do komunikacji jest zawsze używany port 443, standardowy dla protokołu HTTPS.

Konsola HMC może się łączyć z Internetem bezpośrednio lub za pośrednictwem serwera proxy dostarczonego przez użytkownika. Decyzja o wyborze jednej z tych możliwości dla konkretnej instalacji zależy od wymaganego przez firmę poziomu bezpieczeństwa i struktury sieci. Podczas nawiązywania połączeń internetowych z szyfrowaniem SSL (bezpośrednio lub poprzez serwer proxy SSL) konsola HMC wykorzystuje adresy podane poniżej.

Wybór protokołu internetowego

Sekcja zawiera informacje na temat określania wersji adresów IP, której będzie używać konsola HMC podczas nawiązywania połączenia z dostawcą usług.

Podczas nawiązywania połączenia z dostawcą usług większość użytkowników korzysta z protokołu IP w wersji 4 (IPv4). Adresy IPv4 używane do nawiązania połączenia z Internetem składają się z czterech bajtów rozdzielonych kropkami (na przykład 9.60.12.123). Do nawiązywania połączenia z dostawcą usług można też używać protokołu IP w wersji 6 (IPv6). Administratorzy sieci często wykorzystują protokół IPv6 w celu zapewnienia unikalnej przestrzeni adresowej. W razie wątpliwości dotyczących wersji protokołu IP używanej w danej instalacji należy skontaktować się z administratorem sieci. Więcej informacji na temat korzystania z obu wersji zawierają sekcje [“Ustawianie adresu IPv4”](#) na stronie 67 i [“Ustawianie adresu IPv6”](#) na stronie 68.

Listy adresów do internetowych połączeń SSL

Sekcja zawiera listę adresów używanych przez konsolę HMC w przypadku łączenia się z Internetem przy użyciu protokołu SSL.

Podczas nawiązywania internetowych połączeń SSL z działem serwisu i wsparcia IBM konsola HMC używa podanych niżej adresów IPv4.

Następujące adresy IPv4 są używane w przypadku wszystkich lokalizacji:

- 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

Adresy IPv4 dla klientów z Ameryk:

- 129.42.160.48
- 129.42.160.49
- 207.25.252.197
- 207.25.252.200
- 207.25.252.204

Następujące adresy IPv4 są używane w przypadku wszystkich lokalizacji znajdujących się poza Amerykami:

- 129.42.160.48
- 129.42.160.50
- 207.25.252.197
- 207.25.252.200
- 207.25.252.205

Uwaga: W przypadku konfigurowania firewalla, aby akceptował połączenia konsoli HMC z tymi serwerami, wymagane są tylko adresy IP dla odpowiedniego regionu geograficznego.

Podczas nawiązywania internetowych połączeń SSL z działem serwisu i wsparcia IBM konsola HMC używa następujących adresów IPv6:

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

Używanie wielu serwerów zgłoszeń automatycznych

Sekcja zawiera informacje potrzebne w sytuacji, gdy mają być wykorzystywane co najmniej dwa serwery zgłoszeń automatycznych.

Aby wyeliminować pojedynczy punkt podatności na awarię, należy skonfigurować konsolę HMC w taki sposób, aby używała wielu serwerów zgłoszeń automatycznych. Próba obsłużenia każdego zdarzenia serwisowego jest podejmowana przez pierwszy dostępny serwer zgłoszeń automatycznych. Jeśli nie powiedzie się połączenie z tym serwerem zgłoszeń automatycznych lub transmisja danych, zgłoszenie serwisowe będzie ponawiane z użyciem kolejnych dostępnych serwerów zgłoszeń automatycznych, do momentu pomyślnego nawiązania połączenia lub wyczerpania listy serwerów.

Problem jest zgłaszany przez podłączoną konsolę HMC, która podczas analizy problemu została zidentyfikowana jako podstawowa konsola analiz dla danego systemu zarządzanego. Ta konsola podstawowa replikuje również raport o problemie na dodatkową konsolę HMC (jeśli została ona zdefiniowana). Konsola dodatkowa musi być rozpoznawana w sieci przez podstawową konsolę HMC. Dodatkowa konsola HMC jest rozpoznawana przez podstawową konsolę HMC jako dodatkowy serwer zgłoszeń automatycznych, gdy:

- Konfiguracja podstawowej konsoli HMC dopuszcza korzystanie z wykrytych serwerów zgłoszeń automatycznych, a docelowy serwer zgłoszeń automatycznych albo znajduje się w tej samej podsieci, co podstawowa konsola HMC, albo zarządza tym samym systemem.

- Serwer zgłoszeń automatycznych został ręcznie dodany do listy konsol z serwerami zgłoszeń automatycznych, za pośrednictwem których można nawiązywać połączenia wychodzące.

Przygotowanie do konfigurowania konsoli HMC

Sekcja zawiera informacje na temat wymaganych ustawień konfiguracyjnych, których znajomość jest niezbędna do rozpoczęcia wykonywania kroków konfiguracji.

Aby skonfigurować konsolę HMC, należy zapoznać się z pojęciami dotyczącymi tego procesu, podjąć odpowiednie decyzje i przygotować właściwe informacje.

W sekcji podano informacje, które będą niezbędne do połączenia konsoli HMC z następującymi miejscami:

- procesorami serwisowymi w systemach zarządzanych,
- partycjami logicznymi na tych systemach zarządzanych,
- zdalnymi stacjami roboczymi,
- serwisem IBM w celu zaimplementowania funkcji zgłoszeń automatycznych.

Aby przygotować konfigurację konsoli HMC, wykonaj następujące kroki:

1. Uzyskaj i zainstaluj najnowszą wersję kodu konsoli HMC, którą zamierzasz zainstalować.
2. Określ położenie fizyczne konsoli HMC w odniesieniu do serwerów, którymi zarządza. Jeśli konsola HMC znajduje się w odległości większej niż 7,6 m (25 stóp) od systemów zarządzanych, należy zapewnić dostęp do konsoli HMC za pośrednictwem przeglądarki WWW z miejsca instalacji systemów zarządzanych, tak aby personel serwisowy miał dostęp do konsoli HMC.
3. Zidentyfikuj serwery, którymi zarządza konsola HMC.
4. Określ, czy do zarządzania serwerami używana jest sieć prywatna, czy otwarta. Jeśli ma być zastosowana sieć prywatna, użyj protokołu DHCP, chyba że jest wykorzystywana konfiguracja CSM (Cluster Systems Management). CSM nie obsługuje protokołu IPv6. Aby uzyskać dostęp do CSM, niezbędne są dwie sieci. Więcej informacji na temat CSM zawiera dokumentacja dostarczona z tą opcją. Więcej informacji na temat sieci prywatnych i otwartych zawiera sekcja [“Wybieranie sieci prywatnej lub otwartej”](#) na stronie 66.
5. Jeśli do zarządzania procesorem FSP używana jest sieć otwarta, należy ręcznie ustawić adres procesora FSP za pomocą menu interfejsu ASMI. Zalecane jest zastosowanie prywatnej, nieroutowalnej sieci.
6. Jeśli używane są dwie konsole HMC, wskaż podstawową i dodatkową konsolę HMC. Podstawowa konsola HMC powinna się znajdować fizycznie bliżej systemu i powinny być na niej skonfigurowane zgłoszenia automatyczne.
7. Określ ustawienia sieciowe niezbędne do połączenia konsoli HMC ze zdalnymi stacjami roboczymi, partycjami logicznymi i urządzeniami sieciowymi.
8. Określ, w jaki sposób konsola HMC będzie przysyłać zgłoszenia automatyczne. Opcje zgłoszeń automatycznych to internetowe połączenia wychodzące z wykorzystaniem protokołu SSL, połączenia modemowe lub połączenia przez sieć VPN.
9. Określ tworzonych użytkowników konsoli HMC, a także ich hasła oraz nadane im role. Użytkownikom **hscroot** i **hscpe** należy przypisać hasło.
10. Przygotuj następujące firmowe informacje kontaktowe, które będą konieczne przy konfigurowaniu zgłoszeń automatycznych:
 - Nazwa firmy
 - Dane kontaktowe administratora
 - Adres poczty elektronicznej
 - Numery telefonów
 - Numery faksów
 - Adres miejsca, w którym znajduje się konsola HMC

11. Jeśli do powiadamiania operatorów lub administratorów systemu o wystąpieniu informacji do serwisu IBM za pomocą zgłoszeń automatycznych ma być wykorzystywana poczta elektroniczna, podaj adres serwera SMTP oraz używane adresy e-mail.
12. Należy zdefiniować następujące hasła:
- Hasło dostępu używane do uwierzytelnienia konsoli HMC na procesorze FSP.
 - Hasło interfejsu ASMI używane przez użytkownika **admin**.
 - Hasło interfejsu ASMI używane przez użytkownika **general**.

Utwórz hasła przy pierwszym połączeniu z nowym serwerem za pośrednictwem konsoli HMC. Jeśli konsola HMC jest nadmiarowa lub jest to druga konsola HMC, uzyskaj hasło użytkownika konsoli HMC i przygotuj się do wprowadzenia go przy pierwszym połączeniu z procesorem FSP serwera zarządzanego.

Po wykonaniu tych kroków przygotowawczych przejdź do czynności przedstawionych w sekcji “Arkusz konfiguracji wstępnej dla konsoli HMC” na stronie 50.

Arkusz konfiguracji wstępnej dla konsoli HMC

Niniejszy arkusz roboczy pozwala przygotować informacje niezbędne do instalacji.

Ulepszona strategia haseł dla konsoli HMC

Nowe hasło trzeba ustawić przy pierwszym użyciu nowo wyprodukowanego serwera z konsolą HMC w wersji 9.940.0 lub nowszej i po przywróceniu ustawień fabrycznych serwera. Ta zmiana strategii pomaga zapewnić, że konsola HMC nie pozostanie w stanie, w którym hasło jest ogólnie znane.

W konsoli HMC w wersji 9.940.0 i nowszych hasło użytkownika `hscroot` jest wygasłe i musi zostać zmienione, zanim użytkownik uzyska dostęp do funkcji konsoli HMC. Więcej informacji na temat sposobu zmiany hasła zawiera sekcja https://www.ibm.com/support/knowledgecenter/POWER9/p9eh6/p9eh6_useridsandpassword.htm. Jednak w przypadku aktualizacji z poprzedniej wersji konsoli HMC lub instalacji operacyjnej nie ma konieczności zmiany hasła.

Ustawienia sieciowe

Interfejs sieci LAN: w tym miejscu należy wybrać dostępne adaptery (na przykład `eth0`, `eth1`), za pomocą których dana konsola HMC będzie się łączyć z systemami zarządzanymi, partycjami logicznymi, serwisem i wsparciem oraz użytkownikami zdalnymi. Więcej informacji na ten temat zawiera sekcja “Połączenia sieciowe konsoli HMC” na stronie 40. Połączenia z konsoli HMC mogą być nawiązywane w sieci prywatnej lub otwartej.

Szybkość i tryb duplexu adaptera Ethernet

W tym miejscu należy wpisać wymaganą szybkość i tryb duplexu adaptera Ethernet. Automatyczne wykrywanie pozwala na określenie optymalnej opcji, gdy nie ma pewności, jaka szybkość i jaki tryb duplexu zapewnią najlepsze rezultaty w przypadku danego sprzętu. Wartość domyślna = Autodetection (Automatyczne wykrywanie). Szybkość nośnika określa szybkość działania adaptera Ethernet w trybie duplexu. Jeśli nie jest konieczne określenie stałej szybkości nośnika, należy wybrać opcję Autodetection (Automatyczne wykrywanie). Każde urządzenie podłączone do procesora FSP (przetłaczniaki/konsola HMC) musi być skonfigurowane w trybie Auto (Speed) / Auto (Duplex), ponieważ jest to domyślne ustawienie dla procesora FSP i nie można go zmieniać.

Tabela 10. Szybkość i tryb duplexu adaptera Ethernet				
Parametr	eth0	eth1	eth2	eth3
Wybierz szybkość i tryb duplexu				

Tabela 10. Szybkość i tryb duplexu adaptera Ethernet (kontynuacja)				
Parametr	eth0	eth1	eth2	eth3
Szybkość nośnika (automatyczne wykrywanie, pełny duplex/ półduplex 10/100/1000)				

Więcej informacji na temat sieci prywatnych i otwartych zawiera sekcja [“Sieci prywatne i otwarte w środowisku konsoli HMC”](#) na stronie 42.

Tabela 11. Sieć prywatna lub otwarta				
Parametr	eth0	eth1	eth2	eth3
Dla każdego adaptera należy określić sieć prywatną (Private) lub otwartą (Open).				

Protokół DHCP (Dynamic Host Configuration Protocol) zapewnia automatyczne, dynamiczne konfigurowanie klientów. Można zdefiniować tę konsolę HMC jako serwer DHCP. Jeśli jest to pierwsza lub jedyna konsola HMC w sieci prywatnej, należy ją skonfigurować jako serwer DHCP. W przypadku włączenia konsoli HMC jako serwera DHCP systemy zarządzane w sieci zostaną automatycznie skonfigurowane i wykryte przez konsolę HMC.

W przypadku adapterów Ethernet skonfigurowanych jako adaptery sieci prywatnej należy wypełnić poniższą tabelę:

Tabela 12. Serwer DHCP		
Parametry	eth0	eth1
Czy chcesz określić tę konsolę HMC jako serwer DHCP? (tak/nie)		
Jeśli tak, zanotuj zakres adresów IP, którego chcesz używać.		

Jeśli używana jest konsola HMC 7063-CR1, należy podłączyć port Ethernet **IPMI** do sieci, aby uzyskać dostęp do kontrolera BMC na konsoli HMC. Więcej informacji na ten temat zawiera sekcja [“Konfigurowanie połączenia z kontrolerem BMC”](#) na stronie 67. Na potrzeby połączenia z kontrolerem BMC należy uzupełnić poniższą tabelę.

Tabela 13. Połączenie z kontrolerem BMC	
Parametry	IPMI
Czy chcesz skonfigurować to połączenie przy użyciu trybu DHCP? (tak/nie)	
Jeśli nie, podaj poniżej odpowiedni adres statyczny:	
Adres IP:	
Maska podsieci:	
Brama:	

W przypadku adapterów Ethernet skonfigurowanych jako adaptery sieci *otwartej* należy wypełnić poniższe tabele. Więcej informacji o różnych wersjach protokołu IP zawiera sekcja [“Konfigurowanie typów sieci konsoli HMC”](#) na stronie 60.

Używany jest protokół IPv6

Jeśli używany jest protokół IPv6, należy w porozumieniu z administratorem sieci ustalić sposób przydzielania adresów IP. Następnie należy wypełnić następujące tabele:

Tabela 14. Protokół IPv6 (statyczny)				
Parametr	eth0	eth1	eth2	eth3
Czy będzie używany statyczny adres IP? Jeśli tak, zapisz tu ten adres.				

Tabela 15. Protokół IPv6 (serwer DHCP)				
Parametr	eth0	eth1	eth2	eth3
Czy adresy IP będą otrzymywane z serwera DHCP? (tak/nie)				

Tabela 16. Protokół IPv6 (router IPv6)				
Parametr	eth0	eth1	eth2	eth3
Czy adresy IP będą otrzymywane z routera IPv6?				

Więcej informacji na temat ustalania adresów IPv6 zawiera sekcja [“Ustawianie adresu IPv6”](#) na stronie 68. Więcej informacji na temat korzystania wyłącznie z adresów IPv6 zawiera sekcja [“Korzystanie wyłącznie z adresów IPv6”](#) na stronie 68.

Używany jest protokół IPv4

Wypełnij poniższe tabele, jeśli używane są adaptery Ethernet skonfigurowane jako adaptery sieci otwartej IPv4.

Tabela 17. Protokół IPv4				
Parametry	eth0	eth1	eth2	eth3
Czy chcesz, aby adres IP był uzyskiwany automatycznie? (tak/nie)				
Jeśli nie, podaj odpowiedni adres poniżej:				
Adres interfejsu TCP/IP:				
Maska sieci interfejsu TCP/IP:				

Tabela 17. Protokół IPv4 (kontynuacja)				
Parametry	eth0	eth1	eth2	eth3
Ustawienia firewalla:				
Czy chcesz skonfigurować ustawienia firewalla konsoli HMC? (tak/nie)				
Jeśli tak, wymień aplikacje i adresy IP, które mają być akceptowane przez firewall:				

Informacje dotyczące protokołu TCP/IP

W przypadku każdego węzła wymagany jest unikalny adres TCP/IP. Dotyczy to zarówno elementów wspomagających, jak i konsoli HMC. Przypisana maska sieci służy do generowania unikalnego adresu, który domyślnie znajduje się w prywatnej sieci LAN. Jeśli węzły są połączone w większą sieć identyfikowaną administrowanym adresem TCP/IP, to można określić adres, który ma być używany. Wartość domyślna jest generowana przez system.

Ustawienia firewalla

Ustawienia firewalla konsoli HMC umożliwiają utworzenie bariery zabezpieczającej, która dopuszcza lub blokuje dostęp do określonych aplikacji sieciowych na konsoli HMC. Ustawienia można konfigurować oddzielnie dla każdego fizycznego interfejsu sieciowego. Pozwala to na kontrolowanie dostępu do określonych aplikacji sieciowych konsoli HMC w poszczególnych sieciach.

Jeśli co najmniej jeden adapter został skonfigurowany jako adapter sieci otwartej, należy podać poniższe informacje dodatkowe, aby umożliwić konsoli HMC uzyskanie dostępu do sieci LAN:

Tabela 18. Adapter sieci otwartej	
Informacje dotyczące hosta lokalnego	
Nazwa hosta konsoli HMC:	
Nazwa domeny:	
Opis konsoli HMC:	
Informacje dotyczące bramy	
Adres bramy: (nnn.nnn.nnn.nnn)	
Urządzenie bramy:	
Udostępnienie usług DNS	
Czy chcesz korzystać z usług DNS? (tak/nie)	
Jeśli tak, wpisz poniżej kolejność przeszukiwania serwerów DNS:	
1.	
2.	
Kolejność przeszukiwania przyrostków domen:	
1.	
2.	

Informacje dotyczące hosta lokalnego

Aby umożliwić identyfikację konsoli HMC w sieci, należy wpisać jej nazwę hosta i nazwę domeny. O ile w sieci nie są wykorzystywane wyłącznie nazwy skrócone, należy wpisać pełną nazwę hosta. Przykładowa nazwa domeny: nazwa.firma.com

Informacje dotyczące bramy

Aby zdefiniować bramę domyślną, należy wpisać adres TCP/IP, który ma być wykorzystywany do routingu pakietów IP. Adres bramy informuje wszystkie komputery i urządzenia sieciowe, kiedy mają być wysyłane dane, jeśli stacja docelowa nie znajduje się w tej samej podsieci co stacja źródłowa.

Udostępnianie usług DNS

System DNS (Domain Name System) umożliwia stosowanie standardowej konwencji nazewnictwa, która ułatwia wyszukiwanie komputerów w sieciach IP. Zdefiniowanie serwerów DNS pozwala na identyfikowanie serwerów i konsoli HMC na podstawie nazw hostów, a nie adresów IP.

Kolejność wyszukiwania serwera DNS

W tym miejscu należy wpisać adresy IP serwerów DNS, które mają być przeszukiwane w celu odwzorowania nazw hostów na adresy IP. Kolejność przeszukiwania można ustawić tylko przy włączonych usługach DNS.

Kolejność wyszukiwania przyrostka domeny

W tym miejscu należy wpisać używane przyrostki domen. Przyrostki te są dodawane przez konsolę HMC do nazw niekwalifikowanych podczas przeszukiwania serwerów DNS. Przyrostki są wyszukiwane w takiej kolejności, w jakiej zostały wpisane. Kolejność przeszukiwania można ustawić tylko przy włączonych usługach DNS.

Powiadomienia pocztą elektroniczną

Aby otrzymywać powiadomienia w przypadku wystąpienia w systemie zdarzeń związanych z problemami sprzętowymi, należy podać adres e-mail.

Tabela 19. Powiadomienia pocztą elektroniczną	
Parametry	Pole wprowadzania
Adresy e-mail:	
Serwer SMTP:	
Port:	
Błędy uwzględniane w powiadomieniach:	
Tylko zdarzenia związane z problemami zgłaszane automatycznie	
Wszystkie zdarzenia związane z problemami	

Serwer SMTP

W tym miejscu należy wpisać adres SMTP serwera używanego do przesyłania powiadomień o zdarzeniach systemowych. Przykładowa nazwa serwera SMTP to relay.us.ibm.com.

SMTP jest protokołem używanym do wysyłania wiadomości e-mail. W przypadku używania protokołu SMTP klient wysyła wiadomość i komunikuje się z serwerem SMTP za pośrednictwem tego protokołu.

Jeśli nie znasz adresu SMTP serwera lub nie masz co do niego pewności, skontaktuj się z administratorem systemu.

Port

W tym miejscu należy wpisać numer portu serwera, na który będą przesyłane powiadomienia o zdarzeniach serwisowych, lub użyć domyślnego portu.

Adresy poczty elektronicznej do powiadamiania

W tym miejscu należy wpisać listę skonfigurowanych adresów poczty elektronicznej, na które będą wysyłane powiadomienia o wystąpieniu zdarzenia systemowego.

- Wybranie opcji **Only call-home problem events** (Tylko zdarzenia związane z problemami zgłaszane automatycznie) pozwala otrzymywać powiadomienia wyłącznie w przypadku, gdy występują zdarzenia zgłaszane automatycznie.
- Wybranie opcji **All problem events** (Wszystkie zdarzenia związane z problemami) pozwala otrzymywać powiadomienia w przypadku wystąpienia dowolnych zdarzeń.

Informacje kontaktowe serwisu

Tabela 20. Informacje kontaktowe serwisu	
Parametry	Pole wprowadzania
Nazwa firmy	
Nazwisko administratora	
Adres poczty elektronicznej	
Numer telefonu	
Alternatywny numer telefonu	
Numer faksu	
Alternatywny numer telefonu	
Ulica i numer	
Ulica i numer 2	
Miasto lub miejscowość	
Stan	
Kod pocztowy	
Kraj lub region	
Lokalizacja konsoli HMC (jeśli taka sama jak powyższy adres administratora, należy wpisać "jw.")	
Ulica i numer	
Ulica i numer 2	
Miasto lub miejscowość	
Stan	
Kod pocztowy	
Kraj lub region	

Autoryzacja serwisu i połączenia serwisowe

Wybierz typ połączenia z dostawcą usług. Opis poszczególnych metod z uwzględnieniem poziomu zabezpieczeń i wymagań konfiguracyjnych zawiera sekcja ["Wybór istniejących serwerów zgłoszeń automatycznych do nawiązywania połączeń z działem serwisu i wsparcia z bieżącej konsoli HMC"](#) na stronie 74.

Tabela 21. Autoryzacja serwisu i połączenia serwisowe	
Parametry	Pole wprowadzania
SSL przez połączenie internetowe	-----

Tabela 21. Autoryzacja serwisu i połączenia serwisowe (kontynuacja)	
Parametry	Pole wprowadzania
Wirtualna sieć prywatna (VPN) przez połączenie internetowe	-----

SSL przez połączenie internetowe:

Jeśli istnieje już połączenie internetowe z konsoli HMC, można go użyć do nawiązania połączenia z dostawcą usług. Połączenie z dostawcą usług można nawiązać bezpośrednio przez istniejące już połączenie internetowe z użyciem szyfrowanego protokołu SSL. Aby skonfigurować obsługę szyfrowanej transmisji SSL w ramach połączenia pośredniego za pomocą serwera proxy SSL, należy wybrać opcję **Użyj serwera proxy SSL**.

Tabela 22. Warstwa SSL	
Parametry	Pole wprowadzania
Czy używać serwera proxy SSL? (tak/nie)	
Jeśli tak, wpisz poniżej odpowiednie informacje:	
Adres:	
Port:	
Czy uwierzytelniać za pomocą serwera proxy SSL?	
Jeśli tak, wpisz poniżej odpowiednie informacje:	
Użytkownik:	
Hasło:	

Protokół używany do połączeń internetowych

Więcej informacji o różnych wersjach protokołu IP zawiera sekcja [“Konfigurowanie typów sieci konsoli HMC”](#) na stronie 60.

- ___ IPv4
- ___ IPv6
- ___ IPv4 i IPv6

Wirtualna sieć prywatna (VPN)

Jeśli istnieje już połączenie internetowe z konsoli HMC, można go użyć do nawiązania połączenia z dostawcą usług. Połączenie z dostawcą usług można nawiązać bezpośrednio, przez istniejące już połączenie internetowe, z użyciem wirtualnej sieci prywatnej (VPN).

Uwaga: Po wybraniu sieci VPN przez połączenie internetowe nie można wybrać żadnych innych opcji.

Serwery zgłoszeń automatycznych

Określ konsole HMC, które mają mieć możliwość łączenia się z działem serwisu i wsparcia jako serwery zgłoszeń automatycznych. Więcej informacji na temat korzystania z wielu serwerów zgłoszeń automatycznych zawiera sekcja [“Używanie wielu serwerów zgłoszeń automatycznych”](#) na stronie 48.

- ___ Ta konsola HMC
- ___ Inna konsola HMC

Jeśli zaznaczono opcję **Inna konsola HMC**, wymień tutaj inne konsole HMC, które zostały skonfigurowane jako serwery zgłoszeń automatycznych:

Tabela 23. Inne konsole HMC, które zostały skonfigurowane jako serwery zgłoszeń automatycznych

Lista nazw hostów lub adresów IP konsoli HMC, które zostały skonfigurowane jako serwery zgłoszeń automatycznych

Dodatkowe korzyści w zakresie wsparcia

Opcje My Systems (Moje systemy) i Premium Search (Wyszukiwanie przekrojowe)

Tabela 24. Opcje My Systems (Moje systemy) i Premium Search (Wyszukiwanie przekrojowe)

Parametry	Pole wprowadzania
Podaj swój identyfikator IBM	_____
Podaj wszelkie inne identyfikatory IBM	_____

Aby można było skorzystać z cennych, spersonalizowanych informacji dotyczących wsparcia, znajdujących się w sekcjach My Systems (Moje systemy) i Premium Search (Wyszukiwanie przekrojowe) w serwisie WWW usług elektronicznych, należy zarejestrować w systemie posiadany identyfikator IBM. Identyfikator IBM można uzyskać po zarejestrowaniu się pod adresem: www.ibm.com/account/profile.

Uwaga: IBM oferuje możliwość personalizowania funkcji dostępnych przez interfejs WWW na podstawie informacji gromadzonych przez aplikację IBM Electronic Service Agent. Aby można było skorzystać z tych funkcji, należy najpierw zarejestrować się w serwisie WWW IBM Registration pod adresem <http://www.ibm.com/account/profile>.

Użytkownicy mogą zostać uprawnieni do korzystania z informacji zebranych za pomocą aplikacji Electronic Service Agent w celu personalizowania funkcji dostępnych w sieci WWW. Przyznanie takiego uprawnienia wymaga wpisania identyfikatora IBM zarejestrowanego w serwisie WWW IBM Registration. Pod adresem <http://www.ibm.com/support/electronic> znajdują się przydatne informacje związane ze wsparciem. Są one dostępne dla klientów, którzy zarejestrowali w systemie identyfikator IBM.

Konfigurowanie konsoli HMC

W rozdziale opisano sposób konfigurowania połączeń sieciowych, bezpieczeństwa, aplikacji serwisowych i niektórych preferencji użytkownika.

W zależności od stopnia indywidualnego dostosowania, które ma być zastosowane w konfiguracji konsoli HMC, istnieje kilka opcji konfigurowania konsoli HMC zgodnie z potrzebami użytkownika. Kreator instalacji z przewodnikiem jest narzędziem dostępnym na konsoli HMC, zaprojektowanym z myślą o ułatwieniu procesu konfigurowania konsoli HMC. Kreator pozwala użytkownikowi szybko skonfigurować zalecane środowisko konsoli HMC albo prowadzi go przez wszystkie dostępne ustawienia. Czynności konfiguracyjne można również wykonać bez pomocy kreatora zgodnie z opisem w sekcji [Konfigurowanie konsoli HMC za pomocą menu HMC](#).

Na wstępie należy zebrać wymagane informacje, które umożliwią pomyślne wykonanie czynności konfiguracyjnych. Listę wymaganych informacji zawiera sekcja [“Przygotowanie do konfigurowania konsoli HMC”](#) na stronie 49. Po zakończeniu przygotowań należy się upewnić, że zostały wykonane czynności, których opis zawiera [“Arkusz konfiguracji wstępnej dla konsoli HMC”](#) na stronie 50, a następnie powrócić do niniejszej sekcji.

Konfigurowanie konsoli HMC za pomocą Kreatora instalacji z przewodnikiem

W większości przypadków konsolę HMC można skonfigurować do wydajnej pracy, wykorzystując wiele spośród dostępnych ustawień domyślnych. Przedstawiona lista kontrolna umożliwia szybkie przygotowanie konsoli HMC do pracy. Po wykonaniu tych kroków konsola HMC będzie skonfigurowana jako serwer DHCP (Dynamic Host Configuration Protocol) w sieci prywatnej (połączonej bezpośrednio).

Konfigurowanie konsoli HMC za pomocą menu

Sekcja zawiera pełną listę czynności konfiguracyjnych konsoli HMC i prowadzi użytkownika przez proces konfigurowania konsoli HMC. Opcję tę należy wybrać, jeśli nie będzie używany Kreator instalacji z przewodnikiem.

Aby ustawienia konfiguracji zostały wprowadzone, należy zrestartować konsolę HMC. Z tego powodu warto wydrukować listę kontrolną, aby można było z niej korzystać podczas dalszego konfigurowania konsoli HMC.

Poniższe informacje są opatrzone odniesieniami do opisów czynności, które nie są zawarte w niniejszym dokumencie. Informacje o sprzęcie IBM Power Systems jest dostępne na konsoli HMC i w sieci WWW. Na konsoli HMC można uzyskać dostęp do Centrum Wiedzy IBM w prawym górnym rogu paska zadań. W sieci WWW Centrum Wiedzy IBM jest dostępne pod adresem <https://www.ibm.com/support/knowledgecenter>.

Poniższe informacje są opatrzone odniesieniami do opisów czynności, które nie są zawarte w niniejszym pliku PDF. Dostęp do dodatkowych materiałów pomocniczych można uzyskać w sekcji **Additional Resources** (Zasoby dodatkowe) na stronie powitalnej konsoli HMC.

Wymagania wstępne

Przed rozpoczęciem konfigurowania konsoli HMC za pomocą menu konsoli HMC należy wykonać działania przygotowawcze konfiguracji, opisane w sekcji [“Przygotowanie do konfigurowania konsoli HMC”](#) na stronie 49.

Tabela 25. Czynności ręcznej konfiguracji konsoli HMC oraz miejsca zawierające informacje pokrewne	
Czynność	Gdzie znaleźć informacje pokrewne
1. Uruchom konsolę HMC.	“Uruchamianie konsoli HMC” na stronie 59
2. Ustaw datę i godzinę.	
3. Zmień predefiniowane hasła.	
4. Utwórz dodatkowe konta użytkowników i powróć do tej listy kontrolnej po zakończeniu tej czynności.	
5. Skonfiguruj połączenia sieciowe.	“Konfigurowanie typów sieci konsoli HMC” na stronie 60
6. W przypadku konsoli HMC model 7063-CR1 skonfiguruj adres IP kontrolera BMC (baseboard management controller).	“Konfigurowanie połączenia z kontrolerem BMC” na stronie 67
7. Jeśli są używane sieć otwarta i stały adres IP, określ informacje identyfikacyjne.	
8. Jeśli są używane sieć otwarta i stały adres IP, skonfiguruj pozycję routingu jako bramę domyślną.	“Konfigurowanie pozycji routingu jako bramy domyślnej” na stronie 70
9. Jeśli są używane sieć otwarta i stały adres IP, skonfiguruj usługi DNS.	“Konfigurowanie usług nazw domen” na stronie 70
10. Jeśli używany jest stały adres IP oraz włączono usługi DNS, skonfiguruj przyrostki domen.	“Konfigurowanie przyrostków domen” na stronie 70

Tabela 25. Czynności ręcznej konfiguracji konsoli HMC oraz miejsca zawierające informacje pokrewne (kontynuacja)

Czynność	Gdzie znaleźć informacje pokrewne
11. Skonfiguruj na serwerze łączenie z serwisem i wsparciem IBM, a po zakończeniu tej czynności powrót do niniejszej listy kontrolnej.	“Konfigurowanie lokalnej konsoli w celu zgłaszania błędów do działu serwisu i wsparcia” na stronie 73
12. Skonfiguruj Menedżera zdarzeń dla zgłoszeń automatycznych.	“Konfigurowanie Menedżera zdarzeń dla zgłoszeń automatycznych” na stronie 76
13. Podłącz system zarządzany do źródła zasilania.	
14. Ustaw hasła dla systemu zarządzanego i wszystkie hasła interfejsu ASMI (ogólne i administratora).	“Ustawianie haseł dla systemu zarządzanego” na stronie 77
15. Uzyskaj dostęp do interfejsu ASMI w celu ustawienia daty i czasu na systemie zarządzanym.	
16. Uruchom system zarządzany, a po zakończeniu tej czynności powrót do niniejszej listy kontrolnej.	
17. Sprawdź, czy w systemie zarządzanym jest jedna partycja logiczna.	
18. Opcjonalnie: dodaj inny system zarządzany, a po zakończeniu tej czynności powrót do niniejszej listy kontrolnej.	
19. Opcjonalnie: jeśli za pomocą konsoli HMC instalowany jest nowy serwer, skonfiguruj partycje logiczne i zainstaluj system operacyjny.	
20. Jeśli nie jest instalowany nowy serwer, wykonaj opcjonalne czynności pokonfiguracyjne, aby dodatkowo dostosować konfigurację.	“Czynności pokonfiguracyjne” na stronie 79

Uruchamianie konsoli HMC

Po zalogowaniu się do konsoli HMC można wybrać język interfejsu użytkownika. Logując się do konsoli HMC po raz pierwszy, należy użyć domyślnego identyfikatora użytkownika `hscroot` z hasłem `abc123`.

O tym zadaniu

Aby uruchomić konsolę HMC, postępuj zgodnie z następującymi instrukcjami:

Procedura

1. Włącz konsolę HMC przez naciśnięcie przycisku zasilania.
2. Jeśli preferujesz język angielski, kontynuuj od kroku 4.
Jeśli preferujesz język inny niż angielski, wpisz liczbę **2**, gdy zostanie wyświetlone pytanie o zmianę ustawień narodowych.
Uwaga: Jeśli nie zareagujesz, pytanie zniknie po 30 sekundach.
3. W oknie **Locale Selection** (Wybór ustawień narodowych) zaznacz na liście ustawienia narodowe, które mają być używane, a następnie kliknij przycisk **OK**. Ustawienia narodowe określają język interfejsu konsoli HMC.
4. Kliknij opcję **Log on and launch the Hardware Management Console web application** (Zaloguj się i uruchom aplikację WWW konsoli HMC).

5. Zaloguj się do konsoli HMC, korzystając z następujących domyślnych identyfikatorów użytkowników i hasel:

Identyfikator: hscroot

Hasło: abc123

HMC Enhanced

Wyświetla nowszy i rozszerzony interfejs GUI z zaawansowanymi opcjami PowerVM.

HMC Classic

Wyświetla standardowy interfejs GUI bez zaawansowanych opcji PowerVM.

Uwaga: Jeśli konsola HMC działa jako serwer DHCP, używa domyślnego hasła przy pierwszym łączeniu się z procesorem serwisowym.

6. Naciśnij klawisz Enter.

Zmiana daty i godziny

Data i godzina w konsoli HMC są odmierzone przez zegar zasilany akumulatorami. Jeśli wymieniano akumulator lub jeśli fizycznie przeniesiono system do innej strefy czasowej, może zaistnieć potrzeba wprowadzenia zmian w ustawieniach daty i godziny konsoli. Sekcja zawiera informacje na temat sposobu zmiany daty i godziny dla konsoli HMC.

O tym zadaniu

Zmiana daty i godziny nie ma wpływu na system i partycje logiczne zarządzane przez konsolę HMC.

Aby zmienić datę i godzinę dla konsoli HMC, wykonaj następujące czynności:

Procedura

1. Sprawdź, czy masz przypisaną jedną z następujących ról:

- Główny administrator
- Przedstawiciel serwisu
- Operator
- Obserwator

2. W obszarze nawigacyjnym kliknij ikonę **HMC Management** (Zarządzanie konsolą HMC) , a następnie wybierz opcję **Console Settings** (Ustawienia konsoli).
3. W panelu zawartości kliknij opcję **Change Date and Time** (Zmiana daty i godziny).
4. Jeśli w polu **Clock** (Zegar) zostanie wybrana opcja **UTC**, ustawienia godziny zostają automatycznie dopasowane do czasu letniego w wybranej przez użytkownika strefie czasowej. Wprowadź datę, godzinę i strefę czasową, a następnie kliknij przycisk **OK**.

Wyniki

Konfigurowanie typów sieci konsoli HMC

W sekcji opisano sposób konfigurowania konsoli HMC tak, aby mogła się komunikować z systemem zarządzanym, partycjami logicznymi, użytkownikami zdalnymi oraz działem serwisu i wsparcia.

Konfigurowanie ustawień konsoli HMC do użycia sieci otwartej w celu połączenia się z systemem zarządzanym

W sekcji opisano sposób konfigurowania konsoli HMC tak, aby mogła się łączyć z systemem zarządzanym i zarządzać nim za pośrednictwem sieci otwartej.

Zanim rozpocznie

Aby skonfigurować ustawienia sieciowe konsoli HMC tak, aby mogła się ona łączyć z systemem zarządzanym za pośrednictwem sieci otwartej, wykonaj następujące czynności:

Tabela 26. Konfigurowanie ustawień konsoli HMC do użycia sieci otwartej w celu połączenia się z systemem zarządzanym	
Czynność	Gdzie znaleźć informacje pokrewne
1. Zdecyduj, który interfejs będzie używany dla systemu zarządzanego. Preferowany jest interfejs eth0 .	"Arkusze konfiguracji wstępnej dla konsoli HMC" na stronie 50
2. Określ porty Ethernet dla konsoli HMC.	"Identyfikowanie portu sieci Ethernet zdefiniowanego jako eth0" na stronie 64
3. Skonfiguruj adapter Ethernet, wykonując następujące czynności:	
a. Ustaw szybkość nośnika.	"Ustawianie szybkości nośników" na stronie 65
b. Wybierz typ sieci otwartej.	"Wybieranie sieci prywatnej lub otwartej" na stronie 66
c. Ustaw adresy statyczne.	"Ustawianie adresu IPv6" na stronie 68
d. Ustaw firewall.	"Zmiana ustawień firewalla konsoli HMC" na stronie 68
e. Skonfiguruj bramę domyślną.	"Konfigurowanie pozycji routingu jako bramy domyślnej" na stronie 70
f. Skonfiguruj usługi DNS.	"Konfigurowanie usług nazw domen" na stronie 70
4. Skonfiguruj dodatkowe adaptory (jeśli istnieją).	
5. Przetestuj połączenie między serwerem zarządzanym i konsolą HMC.	"Testowanie połączenia między konsolą HMC a systemem zarządzanym" na stronie 78

Konfigurowanie ustawień konsoli HMC do użycia sieci prywatnej w celu połączenia się z systemem zarządzanym

W sekcji opisano sposób konfigurowania konsoli HMC tak, aby mogła się łączyć z systemem zarządzanym i zarządzać nim za pośrednictwem sieci prywatnej.

Zanim rozpocznie

Aby skonfigurować ustawienia sieciowe konsoli HMC tak, aby mogła się ona łączyć z systemem zarządzanym za pośrednictwem sieci prywatnej, wykonaj następujące czynności:

Tabela 27. Konfigurowanie ustawień konsoli HMC do użycia sieci prywatnej w celu połączenia się z systemem zarządzanym	
Czynność	Gdzie znaleźć informacje pokrewne
1. Zdecyduj, który interfejs będzie używany dla systemu zarządzanego.	"Arkusze konfiguracji wstępnej dla konsoli HMC" na stronie 50
2. Określ porty Ethernet dla konsoli HMC.	"Identyfikowanie portu sieci Ethernet zdefiniowanego jako eth0" na stronie 64
3. Skonfiguruj konsolę HMC jako serwer DHCP.	"Konfigurowanie konsoli HMC jako serwera DHCP" na stronie 66

Tabela 27. Konfigurowanie ustawień konsoli HMC do użycia sieci prywatnej w celu połączenia się z systemem zarządzanym (kontynuacja)

Czynność	Gdzie znaleźć informacje pokrewne
4. Przetestuj połączenie między serwerem zarządzanym i konsolą HMC.	“Testowanie połączenia między konsolą HMC a systemem zarządzanym” na stronie 78

Konfigurowanie ustawień konsoli HMC do użycia sieci otwartej w celu połączenia się z partycjami logicznymi

Zanim rozpocznesz

Aby skonfigurować ustawienia sieciowe konsoli HMC tak, aby mogła się ona łączyć z partycjami logicznymi za pośrednictwem sieci otwartej, wykonaj następujące czynności:

Tabela 28. Konfigurowanie ustawień konsoli HMC do użycia sieci otwartej w celu połączenia się z partycjami logicznymi

Czynność	Gdzie znaleźć informacje pokrewne
1. Zdecyduj, który interfejs będzie używany dla systemu zarządzanego.	“Arkusze konfiguracji wstępnej dla konsoli HMC” na stronie 50
2. Określ porty Ethernet dla konsoli HMC.	“Identyfikowanie portu sieci Ethernet zdefiniowanego jako eth0” na stronie 64
3. Skonfiguruj adapter Ethernet, wykonując następujące czynności:	
a. Ustaw szybkość nośnika.	“Ustawianie szybkości nośników” na stronie 65
b. Wybierz typ sieci otwartej.	“Wybieranie sieci prywatnej lub otwartej” na stronie 66
c. Ustaw adresy statyczne.	“Ustawianie adresu IPv6” na stronie 68
d. Ustaw firewall.	“Zmiana ustawień firewalla konsoli HMC” na stronie 68
e. Skonfiguruj bramę domyślną.	“Konfigurowanie pozycji routingu jako bramy domyślnej” na stronie 70
f. Skonfiguruj usługi DNS.	“Konfigurowanie usług nazw domen” na stronie 70
4. Skonfiguruj dodatkowe adaptory (jeśli istnieją).	
5. Przetestuj połączenie między serwerem zarządzanym i konsolą HMC.	“Testowanie połączenia między konsolą HMC a systemem zarządzanym” na stronie 78

Konfigurowanie ustawień konsoli HMC do użycia sieci otwartej w celu połączenia się z użytkownikami zdalnymi

Zanim rozpocznesz

Aby skonfigurować ustawienia sieciowe konsoli HMC tak, aby mogła się ona łączyć z użytkownikami zdalnymi za pośrednictwem sieci otwartej, wykonaj następujące czynności:

Tabela 29. Konfigurowanie ustawień konsoli HMC do użycia sieci otwartej w celu połączenia się z użytkownikami zdalnymi

Czynność	Gdzie znaleźć informacje pokrewne
1. Zdecyduj, który interfejs będzie używany dla systemu zarządzanego.	“Arkusze konfiguracji wstępnej dla konsoli HMC” na stronie 50
2. Określ porty Ethernet dla konsoli HMC.	“Identyfikowanie portu sieci Ethernet zdefiniowanego jako eth0” na stronie 64
3. Skonfiguruj adapter Ethernet, wykonując następujące czynności:	
a. Ustaw szybkość nośnika.	“Ustawianie szybkości nośników” na stronie 65
b. Wybierz typ sieci otwartej.	“Wybieranie sieci prywatnej lub otwartej” na stronie 66
c. Ustaw adresy statyczne.	“Ustawianie adresu IPv6” na stronie 68
d. Ustaw firewall.	“Zmiana ustawień firewalla konsoli HMC” na stronie 68
e. Skonfiguruj bramę domyślną.	“Konfigurowanie pozycji routingu jako bramy domyślnej” na stronie 70
f. Skonfiguruj usługi DNS.	“Konfigurowanie usług nazw domen” na stronie 70
g. Skonfiguruj przyrostki.	“Konfigurowanie przyrostków domen” na stronie 70
4. Skonfiguruj dodatkowe adaptory (jeśli istnieją).	

Konfigurowanie ustawień serwera zgłoszeń automatycznych na konsoli HMC

Zanim rozpoczniesz

Aby skonfigurować serwer zgłoszeń automatycznych na konsoli HMC w sposób umożliwiający zgłaszanie problemów, wykonaj następujące czynności:

Tabela 30. Konfigurowanie ustawień serwera zgłoszeń automatycznych na konsoli HMC

Czynność	Gdzie znaleźć informacje pokrewne
1. Upewnij się, że dysponujesz wszystkimi potrzebnymi informacjami o kliencie	“Arkusze konfiguracji wstępnej dla konsoli HMC” na stronie 50
2. Skonfiguruj zgłaszanie błędów przez bieżącą konsolę HMC lub wybierz istniejący serwer zgłoszeń automatycznych, za pośrednictwem którego będą zgłaszane błędy	“Konfigurowanie lokalnej konsoli w celu zgłaszania błędów do działu serwisu i wsparcia” na stronie 73 “Wybór istniejących serwerów zgłoszeń automatycznych do nawiązywania połączeń z działem serwisu i wsparcia z bieżącej konsoli HMC” na stronie 74
3. Sprawdź, czy konfiguracja zgłoszeń automatycznych jest prawidłowa	“Sprawdzanie poprawnego działania połączenia z działem serwisu i wsparcia” na stronie 75
4. Nadaj użytkownikom uprawnienia do przeglądania zgromadzonych danych o systemie	“Nadawanie użytkownikom uprawnień do przeglądania zgromadzonych danych o systemie” na stronie 75

Tabela 30. Konfigurowanie ustawień serwera zgłoszeń automatycznych na konsoli HMC (kontynuacja)	
Czynność	Gdzie znaleźć informacje pokrewne
5. Zaplanuj przesyłanie danych o systemie	"Przesyłanie informacji serwisowych" na stronie <u>76</u>

Identyfikowanie portu sieci Ethernet zdefiniowanego jako eth0

Do utworzenia połączenia z serwerem zarządzanym należy użyć portu sieci Ethernet zdefiniowanego jako eth0 na konsoli HMC.

Jeśli w gniazdach PCI na konsoli HMC nie zainstalowano dodatkowych adapterów Ethernet, a konsola HMC ma być używana jako serwer DHCP dla systemów zarządzanych, podstawowy zintegrowany port Ethernet będzie na konsoli HMC zawsze zdefiniowany jako port eth0 lub eth1.

Jeśli w gniazdach PCI zostaną zainstalowane dodatkowe adaptory Ethernet, zidentyfikowanie portu zdefiniowanego jako eth0 będzie zależać od położenia i typu zainstalowanych adapterów Ethernet.

Uwaga: Poniższe reguły ogólne mogą nie mieć zastosowania do wszystkich konfiguracji.

Poniższa tabela zawiera opis reguł rozmieszczania adapterów Ethernet według typu konsoli HMC.

Tabela 31. Typy konsoli HMC i związane z nimi reguły rozmieszczenia adapterów Ethernet	
Typ konsoli HMC	Reguły rozmieszczenia adapterów Ethernet
Stelażowe konsole HMC z dwoma zintegrowanymi portami Ethernet.	Konsola HMC obsługuje tylko jeden dodatkowy adapter Ethernet. • Jeśli zostanie zainstalowany dodatkowy adapter Ethernet, jego port będzie zdefiniowany jako eth0. W takim przypadku podstawowy zintegrowany port sieci Ethernet będzie zdefiniowany jako eth1, a dodatkowy zintegrowany port sieci Ethernet jako eth2. • Jeśli używany jest dwuportowy adapter Ethernet, portem eth0 będzie port oznaczony Act/Link A. Port oznaczony Act/link B jest portem eth1. W takim przypadku podstawowy zintegrowany port Ethernet będzie zdefiniowany jako eth2, a dodatkowy zintegrowany port sieci Ethernet jako eth3. • Jeśli nie zostanie zainstalowany żaden adapter, podstawowy zintegrowany port sieci Ethernet będzie zdefiniowany jako eth0.

Tabela 31. Typy konsoli HMC i związane z nimi reguły rozmieszczenia adapterów Ethernet (kontynuacja)

Typ konsoli HMC	Reguły rozmieszczenia adapterów Ethernet
Modele autonomiczne z jednym zintegrowanym portem Ethernet.	Definicje portów zależą od typu zainstalowanego adaptera Ethernet: • Jeśli zainstalowany jest tylko jeden adapter Ethernet, będzie on zdefiniowany jako eth0. • Jeśli używany jest dwuportowy adapter Ethernet, portem eth0 będzie port oznaczony Act/link A. Port oznaczony Act/link B będzie wtedy portem eth1. W takim przypadku podstawowy zintegrowany port Ethernet będzie zdefiniowany jako eth2. • Jeśli nie zostanie zainstalowany żaden adapter, podstawowy zintegrowany port sieci Ethernet będzie zdefiniowany jako eth0. • Jeśli zainstalowano wiele adapterów Ethernet, należy zapoznać się z sekcją "Określanie nazwy interfejsu adaptera Ethernet" na stronie 65.

Określanie nazwy interfejsu adaptera Ethernet

Jeśli konsola HMC jest skonfigurowana jako serwer DHCP, serwer ten może działać wyłącznie na złączach kart sieciowych, które konsola HMC zidentyfikuje jako eth0 i eth1. Może też być konieczne określenie złącza karty sieciowej, do którego należy podłączyć kabel Ethernet. Sekcja zawiera informacje na temat określania, które złącza kart sieciowych są przez konsolę HMC identyfikowane jako eth0 i eth1.

O tym zadaniu

Aby określić nazwę, którą konsola HMC przypisała adapterowi Ethernet, wykonaj następujące kroki:

Procedura

1. W obszarze nawigacyjnym kliknij ikonę **HMC Management** (Zarządzanie konsolą HMC) , a następnie wybierz opcję **Console Settings** (Ustawienia konsoli).
2. W panelu zawartości kliknij opcję **Change Network Settings** (Zmiana ustawień sieciowych).
3. W oknie **Change Network Settings** (Zmiana ustawień sieciowych) kliknij kartę **LAN adapters** (Adaptory LAN). Następujący przykładowy wpis wskazuje, że port Ethernet został zidentyfikowany jako eth0: Ethernet eth0 52:54:00:fa:b6:8e (<adres IP konsoli HMC>).
4. Zapisz wyniki. Aby wyświetlić lub zmienić ustawienia adaptera sieci LAN, kliknij opcję **Details** (Szczegóły).
5. Kliknij przycisk **OK**.

Ustawianie szybkości nośników

Sekcja zawiera informacje na temat określania szybkości nośnika, w tym szybkości oraz trybu duplex adaptera Ethernet.

Zanim rozpoczniesz

Domyślną wartością ustawień adaptera konsoli HMC jest **Autodetection** (Automatyczne wykrywanie). Jeśli adapter jest podłączony do przełącznika sieci LAN, należy ustawić wartości zgodne z ustawieniami portów przełącznika. Aby ustawić szybkość i tryb duplex nośnika, wykonaj następujące czynności:

Procedura

1. W obszarze nawigacyjnym kliknij ikonę **HMC Management** (Zarządzanie konsolą HMC) , a następnie wybierz opcję **Console Settings** (Ustawienia konsoli).
2. W panelu zawartości kliknij opcję **Change network settings** (Zmiana ustawień sieciowych).
3. Kliknij zakładkę **LAN Adapters** (Adaptery sieci LAN).
4. Zaznacz odpowiedni adapter LAN, a następnie kliknij opcję **Details** (Szczegóły).
5. W sekcji z informacjami dotyczącymi sieci lokalnej (LAN) wybierz opcję **Autodetection** (Automatyczne wykrywanie) lub zaznacz odpowiednią kombinację szybkości nośnika i trybu duplex.
6. Kliknij przycisk **OK**.

Wybieranie sieci prywatnej lub otwartej

Prywatną sieć serwisową tworzy konsola HMC razem z systemami zarządzanymi. Prywatna sieć serwisowa jest ograniczona do konsol i systemów przez nie zarządzanych i jest oddzielona od sieci przedsiębiorstwa. Sieć otwartą tworzy prywatna sieć serwisowa razem z siecią przedsiębiorstwa. Oprócz konsol i systemów zarządzanych sieć otwarta może zawierać sieciowe punkty końcowe i może obejmować wiele podsieci i urządzeń sieciowych.

O tym zadaniu

Aby wybrać sieć prywatną lub publiczną, wykonaj następujące kroki:

Procedura

1. W obszarze nawigacyjnym kliknij ikonę **HMC Management** (Zarządzanie konsolą HMC) , a następnie wybierz opcję **Console Settings** (Ustawienia konsoli).
2. W panelu zawartości kliknij opcję **Change network settings** (Zmiana ustawień sieciowych).
3. Kliknij zakładkę **LAN Adapters** (Adaptery sieci LAN).
4. Zaznacz odpowiedni adapter LAN, a następnie kliknij opcję **Details** (Szczegóły).
5. Kliknij kartę **LAN Adapter** (Adapter sieci LAN).
6. Na stronie informacyjnej sieci lokalnej zaznacz opcję **Private** (Prywatna) lub **Open** (Otwarta).
7. Kliknij przycisk **OK**.

Konfigurowanie konsoli HMC jako serwera DHCP

Protokół DHCP (Dynamic Host Configuration Protocol) zapewnia automatyczne, dynamiczne konfigurowanie klientów.

Aby skonfigurować konsolę HMC jako serwer DHCP, wykonaj następujące kroki:

1. W obszarze nawigacyjnym kliknij ikonę **HMC Management** (Zarządzanie konsolą HMC) , a następnie wybierz opcję **Console Settings** (Ustawienia konsoli).
2. W panelu zawartości kliknij opcję **Change network settings** (Zmiana ustawień sieciowych). Zostanie otwarte okno Customize Network Settings (Dostosuj ustawienia sieciowe).
3. Zaznacz odpowiedni adapter LAN, a następnie kliknij opcję **Details** (Szczegóły).
4. Wybierz opcję **Private** (Prywatna), a następnie wybierz typ sieci.
5. W sekcji DHCP Server (Serwer DHCP) wybierz opcję **Enable DHCP Server** (Włącz serwer DHCP), aby aktywować konsolę HMC jako serwer DHCP.

Uwaga: Skonfigurowanie konsoli HMC jako serwera DHCP jest możliwe tylko w sieci prywatnej. Jeśli używana jest sieć otwarta, opcja **Enable DHCP** jest niedostępna.

6. Wprowadź zakres adresów serwera DHCP.

7. Kliknij przycisk **OK**.

Jeśli konsola HMC została skonfigurowana w ten sposób, że jest serwerem DHCP w sieci prywatnej, należy sprawdzić, czy prywatna sieć DHCP dla konsoli HMC została poprawnie skonfigurowana. Informacje dotyczące podłączania konsoli HMC do sieci prywatnej zawiera sekcja [“Wybieranie sieci prywatnej lub otwartej”](#) na stronie 66.

Więcej informacji zawiera sekcja [“Konsola HMC jako serwer DHCP”](#) na stronie 43.

Konfigurowanie połączenia z kontrolerem BMC

Istnieje możliwość wyświetlenia i skonfigurowania ustawień sieciowych kontrolera BMC na potrzeby konsoli zarządzania.

Uwaga: To zadanie ma zastosowanie wyłącznie do systemu 7063-CR1. To połączenie jest wymagane do uzyskania dostępu do kontrolera BMC (baseboard management controller) na konsoli HMC.

Aby skonfigurować połączenie z kontrolerem BMC, wykonaj następujące kroki:

1. W obszarze nawigacyjnym kliknij ikonę **HMC Management** (Zarządzanie konsolą HMC) , a następnie wybierz opcję **Console Settings** (Ustawienia konsoli).
2. W panelu zawartości kliknij opcję **Change BMC/IPMI network settings** (Zmień ustawienia sieciowe BMC/IPMI).
3. Wybierz tryb połączenia **DHCP** lub **Static** (Statyczny).

W przypadku wybrania trybu **Static** (Statyczny) wprowadź następujące adresy:

- **IP address** (Adres IP)
- **Subnet mask** (Maska podsieci)
- **Gateway** (Brama)

4. Kliknij przycisk **OK**.

Połączenie sieciowe z kontrolerem BMC można także skonfigurować za pomocą interfejsu programu ładującego Petitboot. Więcej informacji na ten temat można znaleźć w serwisie [Configuring the firmware IP address](#) (Konfigurowanie adresu IP oprogramowania wbudowanego).

Ustawianie adresu IPv4

Sekcja zawiera informacje na temat ustawiania adresu IPv4 dla konsoli HMC.

Procedura

1. W obszarze nawigacyjnym kliknij ikonę **HMC Management** (Zarządzanie konsolą HMC) , a następnie wybierz opcję **Console Settings** (Ustawienia konsoli).
2. W panelu zawartości kliknij opcję **Change network settings** (Zmiana ustawień sieciowych).
3. Kliknij zakładkę **LAN Adapters** (Adaptory sieci LAN).
4. Zaznacz odpowiedni adapter LAN, a następnie kliknij opcję **Details** (Szczegóły).
5. Kliknij zakładkę **Basic Settings** (Ustawienia podstawowe).
6. Wybierz adres IPv4.
7. Jeśli wybrano określenie adresu IP, wpisz adres interfejsu TCP/IP oraz maskę sieci interfejsu TCP/IP.
8. Kliknij przycisk **OK**.

Ustawianie adresu IPv6

Sekcja zawiera informacje na temat ustawiania adresu IPv6 dla konsoli HMC.

Procedura

1. W obszarze nawigacyjnym kliknij ikonę **HMC Management** (Zarządzanie konsolą HMC) , a następnie wybierz opcję **Console Settings** (Ustawienia konsoli).
2. W panelu zawartości kliknij opcję **Change network settings** (Zmiana ustawień sieciowych).
3. Kliknij zakładkę **LAN Adapters** (Adaptery sieci LAN).
4. Zaznacz odpowiedni adapter LAN, a następnie kliknij opcję **Details** (Szczegóły).
5. Kliknij zakładkę **IPv6 Settings** (Ustawienia IPv6).
6. Wybierz opcję **Autoconfig** (Automatyczna konfiguracja) lub dodaj statyczny adres IP.
7. Jeśli został dodany adres IP, wprowadź adres IPv6 oraz długość prefiksu i kliknij przycisk **OK**.
8. Kliknij przycisk **OK**.

Korzystanie wyłącznie z adresów IPv6

Sekcja zawiera informacje na temat skonfigurowania konsoli HMC tak, aby korzystała wyłącznie z adresów IPv6.

Procedura

1. W obszarze nawigacyjnym kliknij ikonę **HMC Management** (Zarządzanie konsolą HMC) , a następnie wybierz opcję **Console Settings** (Ustawienia konsoli).
2. W panelu zawartości kliknij opcję **Change network settings** (Zmiana ustawień sieciowych).
3. Kliknij zakładkę **LAN Adapters** (Adaptery sieci LAN).
4. Zaznacz odpowiedni adapter LAN, a następnie kliknij opcję **Details** (Szczegóły).
5. Wybierz opcję **No IPv4 address** (Nie używaj adresu IPv4).
6. Kliknij zakładkę **IPv6 Settings** (Ustawienia IPv6).
7. Wybierz opcję **Use DHCPv6 to configure IP settings** (Korzystaj z DHCPv6 do konfiguracji ustawień IP) lub dodaj statyczne adresy IP, a następnie kliknij przycisk **OK**.

Co dalej

Po naciśnięciu przycisku **OK** należy zrestartować konsolę HMC, aby wprowadzić zmiany.

Zmiana ustawień firewalla konsoli HMC

W sieci otwartej dostęp do sieci przedsiębiorstwa z zewnątrz jest kontrolowany przez firewall. Także konsola HMC ma firewall na każdym swoim adapterze Ethernet. Jeśli konieczne jest zdalne kontrolowanie konsoli HMC lub umożliwienie innym zdalnego dostępu, należy zmienić ustawienia firewalla na adapterze Ethernet konsoli HMC, która jest podłączona do sieci otwartej.

O tym zadaniu

Aby skonfigurować firewall, wykonaj następujące czynności:

Procedura

1. W obszarze nawigacyjnym kliknij ikonę **HMC Management** (Zarządzanie konsolą HMC) , a następnie wybierz opcję **Console Settings** (Ustawienia konsoli).

2. W panelu zawartości kliknij opcję **Change network settings** (Zmiana ustawień sieciowych).
3. Kliknij zakładkę **LAN Adapters** (Adaptory sieci LAN).
4. Zaznacz odpowiedni adapter LAN, a następnie kliknij opcję **Details** (Szczegóły).
5. Kliknij zakładkę **Firewall**.
6. Wymienione niżej metody umożliwiają takie zdefiniowanie parametrów firewalla, aby akceptował dowolny adres IP używany przez określoną aplikację, lub określenie jednego lub większej liczby dopuszczalnych adresów IP.
 - Aby firewall akceptował każdy adres IP używany przez określoną aplikację:
 - a. W górnym polu wyróżnij aplikację.
 - b. Kliknij **Allow Incoming** (Zezwalaj na przychodzące). Nazwa aplikacji zostanie wyświetlona w dolnym polu, co oznacza, że aplikacja została wybrana.
 - Określ adresy IP, które będą akceptowane przez firewall:
 - a. W górnym polu wyróżnij aplikację.
 - b. Kliknij opcję **Allow Incoming by IP Address** (Zezwalaj na przychodzące wg adresu IP).
 - c. W oknie Hosts Allowed (Dozwolone hosty) wprowadź adres IP i maskę sieci.
 - d. Kliknij opcję **Add** (Dodaj) i kliknij przycisk **OK**.
7. Kliknij przycisk **OK**.

Włączanie zdalnego dostępu do powłoki ograniczonej

Podczas konfigurowania firewalla można włączyć zdalny dostęp do powłoki ograniczonej.

O tym zadaniu

Aby włączyć zdalny dostęp do powłoki ograniczonej, wykonaj następujące kroki:

Procedura

1. W obszarze nawigacyjnym kliknij opcję **HMC Management** (Zarządzanie konsolą HMC).
2. Kliknij opcję **Remote Command Execution** (Zdalne wykonanie komendy).
3. Wybierz opcję **Enable remote command execution using the ssh facility** (Włącz wykonywanie zdalnych komend przy użyciu komendy ssh), a następnie kliknij przycisk **OK**.

Co dalej

Zdalny dostęp do powłoki ograniczonej jest włączony.

Włączanie zdalnego dostępu przez sieć WWW

Można włączyć zdalny dostęp do konsoli HMC.

O tym zadaniu

Aby włączyć zdalny dostęp przez sieć WWW, wykonaj następujące kroki:

Procedura

1. W obszarze nawigacyjnym kliknij opcję **HMC Management** (Zarządzanie konsolą HMC).
2. Kliknij opcję **Remote Operation** (Operacja zdalna).
3. Wybierz opcję **Enabled** (Włączona), a następnie kliknij przycisk **OK**.

Co dalej

Zdalny dostęp przez sieć WWW jest włączony.

Konfigurowanie pozycji routingu jako bramy domyślnej

Sekcja zawiera informacje na temat konfigurowania pozycji routingu jako bramy domyślnej. Ta czynność jest dostępna podczas korzystania z sieci otwartej.

Zanim rozpoczniesz

Aby skonfigurować pozycję routingu jako bramę domyślną, wykonaj następujące kroki:

Procedura

1. W obszarze nawigacyjnym kliknij ikonę **HMC Management** (Zarządzanie konsolą HMC) , a następnie wybierz opcję **Console Settings** (Ustawienia konsoli).
2. W panelu zawartości kliknij opcję **Change network settings** (Zmiana ustawień sieciowych). Zostanie otwarte okno Customize Network Settings (Dostosuj ustawienia sieciowe).
3. Kliknij zakładkę **Routing**.
4. W sekcji informacyjnej bramy domyślnej wpisz adres bramy i urządzenie bramy dla tej pozycji routingu, która ma być bramą domyślną.
5. Kliknij przycisk **OK**.

Konfigurowanie usług nazw domen

Jeśli planowane jest skonfigurowanie sieci otwartej, należy skonfigurować usługi nazw domen.

O tym zadaniu

Jeśli planowane jest skonfigurowanie sieci otwartej, należy skonfigurować usługi nazw domen. System DNS jest systemem rozproszonych baz danych zarządzającym nazwami hostów i przypisanymi do nich adresami IP. Konfiguracja usług nazw domen obejmuje aktywowanie serwera DNS i określenie porządku wyszukiwania przyrostków domen.

Procedura

1. W obszarze nawigacyjnym kliknij ikonę **HMC Management** (Zarządzanie konsolą HMC) , a następnie wybierz opcję **Console Settings** (Ustawienia konsoli).
2. W panelu zawartości kliknij opcję **Change network settings** (Zmiana ustawień sieciowych). Zostanie otwarte okno Change Network Settings (Zmiana ustawień sieciowych).
3. Kliknij zakładkę **Name Services** (Usługi nazw).
4. Aby aktywować usługi DNS, wybierz opcję **DNS enabled** (Usługa DNS jest włączona).
5. Określ kolejność przeszukiwania serwerów DNS oraz przyrostków domen i kliknij przycisk **Add** (Dodaj).
6. Kliknij przycisk **OK**.

Konfigurowanie przyrostków domen

Lista przyrostków domen jest używana do rozstrzygania adresu IP, poczynawszy od pierwszej pozycji na liście.

O tym zadaniu

Przyrostek domeny to łańcuch dołączany do nazwy hosta, który pomaga w ustaleniu jego adresu IP. Mogą na przykład wystąpić problemy z ustaleniem adresu IP hosta moja-nazwa. Jeśli jednak łańcuch moja-lokalizacja.moja-firma.com znajduje się wśród elementów tabeli przyrostków domeny, zostanie podjęta próba rozstrzygnięcia nazwy moja-nazwa.moja-lokalizacja.moja-firma.com.

Aby skonfigurować pozycję przyrostka domeny, wykonaj następujące kroki:

Procedura



1. W obszarze nawigacyjnym kliknij ikonę **HMC Management** (Zarządzanie konsolą HMC), a następnie wybierz opcję **Console Settings** (Ustawienia konsoli).
2. W panelu zawartości kliknij opcję **Change network settings** (Zmiana ustawień sieciowych). Zostanie otwarte okno Customize Network Settings (Dostosuj ustawienia sieciowe).
3. Kliknij zakładkę **Name Services** (Usługi nazw).
4. Wprowadź łańcuch, który ma być używany jako przyrostek domeny.
5. Kliknij opcję **Add** (Dodaj), aby dodać go do listy.

Konfigurowanie konsoli HMC do użycia zdalnego uwierzytelniania LDAP

Konsolę HMC można skonfigurować w taki sposób, aby korzystała ze zdalnego uwierzytelniania przez protokół LDAP (Lightweight Directory Access Protocol).

Zanim rozpoczniesz

Gdy użytkownik loguje się do konsoli HMC, uwierzytelnianie jest w pierwszej kolejności wykonywane przy użyciu lokalnego pliku hasel. Jeśli lokalny plik hasel nie zostanie znaleziony, konsola HMC może nawiązać kontakt ze zdalnym serwerem LDAP, aby przeprowadzić uwierzytelnianie. W tym celu należy skonfigurować konsolę HMC w taki sposób, aby korzystała ze zdalnego uwierzytelniania poprzez protokół LDAP.

Uwaga: Przed skonfigurowaniem na konsoli HMC zdalnego uwierzytelniania LDAP należy się upewnić, że między konsolą HMC a serwerami LDAP istnieje działające połączenie sieciowe. Więcej informacji na temat konfigurowania połączeń sieciowych konsoli HMC zawiera sekcja [“Konfigurowanie typów sieci konsoli HMC”](#) na stronie 60.

O tym zadaniu

Aby skonfigurować na konsoli HMC uwierzytelnianie LDAP, wykonaj następujące kroki:

Procedura



1. W obszarze nawigacyjnym kliknij ikonę **Users and Security** (Użytkownicy i bezpieczeństwo), a następnie wybierz opcję **Systems and Console Security** (Bezpieczeństwo systemów i konsoli).
2. W panelu zawartości wybierz opcję **Manage LDAP** (Zarządzanie serwerem LDAP). Zostanie otwarte okno LDAP Server Definition (Definicja serwera LDAP).
3. Wybierz opcję **Enable LDAP** (Włącz LDAP).
4. Zdefiniuj serwer LDAP, który będzie używany do uwierzytelniania.
5. Zdefiniuj atrybut LDAP używany do identyfikacji uwierzytelnianego użytkownika. Domyślnie jest to **uid**, ale można też używać własnych atrybutów.
6. Zdefiniuj drzewo nazw wyróżniających serwera LDAP (zwane również bazą wyszukiwania).
7. Kliknij przycisk **OK**.
8. Aby użytkownik mógł korzystać z uwierzytelniania LDAP, należy w konfiguracji profilu tego użytkownika włączyć opcję zdalnego uwierzytelniania LDAP zamiast uwierzytelniania lokalnego.

Konfigurowanie konsoli HMC na potrzeby zdalnego uwierzytelniania Kerberos przy użyciu serwerów KDC

Możliwe jest takie skonfigurowanie konsoli HMC, aby korzystała z serwerów centrum dystrybucji kluczy (key distribution center – KDC) do zdalnego uwierzytelniania Kerberos.

Zanim rozpoczniesz

Gdy użytkownik loguje się do konsoli HMC, uwierzytelnianie jest w pierwszej kolejności weryfikowane względem lokalnego pliku hasel. Jeśli lokalny plik hasel nie zostanie znaleziony, konsola HMC może nawiązać kontakt ze zdalnym serwerem Kerberos, aby przeprowadzić uwierzytelnianie. W tym celu należy skonfigurować konsolę HMC w taki sposób, aby korzystała ze zdalnego uwierzytelniania poprzez protokół Kerberos.

Uwaga: Przed skonfigurowaniem na konsoli HMC zdalnego uwierzytelniania Kerberos przy użyciu serwerów KDC należy się upewnić, że między konsolą HMC a serwerami KDC istnieje działające połączenie sieciowe. Więcej informacji na temat konfigurowania połączeń sieciowych konsoli HMC zawiera sekcja [“Konfigurowanie typów sieci konsoli HMC” na stronie 60.](#)

O tym zadaniu

Aby skonfigurować na konsoli HMC zdalne uwierzytelnianie Kerberos z wykorzystaniem serwerów KDC, wykonaj następujące kroki:

Procedura

1. Włącz na konsoli HMC usługę Network Time Protocol (NTP), a następnie ustaw na konsoli HMC i serwerach KDC synchronizowanie czasu z tym samym serwerem NTP. Aby włączyć usługę NTP na konsoli HMC, wykonaj następujące kroki:
 - a) W obszarze nawigacyjnym kliknij ikonę **HMC Management** (Zarządzanie konsolą HMC) , a następnie wybierz opcję **Console Settings** (Ustawienia konsoli).
 - b) W panelu zawartości wybierz opcję **Change Date and Time** (Zmiana daty i godziny).
 - c) Wybierz kartę **NTP Configuration** (Konfiguracja NTP).
 - d) Wybierz opcję **Enable NTP service on this HMC** (Włącz usługę NTP na tej konsoli HMC).
 - e) Kliknij przycisk **OK**.
2. W każdym profilu zdalnego użytkownika konsoli HMC włącz uwierzytelnianie zdalne Kerberos zamiast uwierzytelniania lokalnego.
3. Opcjonalnie, do bieżącej konsoli HMC można zaimportować plik klucza usługi. Plik klucza usługi zawiera nazwę hosta, która będzie używana do identyfikacji konsoli HMC na serwerze KDC. Pliki kluczy usług są zwane również plikami *keytab*. Aby zaimportować plik klucza usługi do tej konsoli HMC, wykonaj następujące kroki:
 - a) W obszarze nawigacyjnym kliknij ikonę **Users and Security** (Użytkownicy i bezpieczeństwo) , a następnie wybierz opcję **Systems and Console Security** (Bezpieczeństwo systemów i konsoli).
 - b) W panelu zawartości wybierz opcję **Manage KDC** (Zarządzanie serwerem KDC).
 - c) Wybierz opcję **Actions > Import Service Key** (Działania > Importuj klucz usługi). Zostanie otwarte okno Import Service Key (Importuj klucz usługi).
 - d) Wpisz lokalizację pliku klucza usługi.
 - e) Kliknij przycisk **OK**.
4. Dodaj nowy serwer KDC do tej konsoli HMC. Aby dodać nowy serwer KDC do tej konsoli HMC, wykonaj następujące kroki:
 - a) W obszarze nawigacyjnym kliknij ikonę **Users and Security** (Użytkownicy i bezpieczeństwo) , a następnie wybierz opcję **Systems and Console Security** (Bezpieczeństwo systemów i konsoli).
 - b) W panelu zawartości wybierz opcję **Manage KDC** (Zarządzanie serwerem KDC).

- c) Wybierz opcję **Actions > Add KDC Server** (Działania > Dodaj serwer KDC). Zostanie otwarte okno Import Service Key (Importuj klucz usługi).
- d) Wpisz dziedzinę i nazwę hosta lub adres IP serwera KDC.
- e) Kliknij przycisk **OK**.

Konfigurowanie lokalnej konsoli w celu zgłaszania błędów do działu serwisu i wsparcia

W sekcji opisano konfigurowanie konsoli HMC w celu automatycznego zgłaszania błędów przez sieć LAN.

Konfigurowanie połączenia konsoli HMC z działem serwisu i wsparcia za pomocą kreatora konfiguracji zgłoszeń automatycznych

Kreator konfiguracji zgłoszeń automatycznych umożliwia skonfigurowanie konsoli HMC jako serwera zgłoszeń automatycznych.

Zanim rozpoczniesz

W procedurze opisano konfigurowanie konsoli HMC jako serwera zgłoszeń automatycznych z wykorzystaniem bezpośredniego (przez sieć LAN) i pośredniego (przez SSL) połączenia z Internetem.

Przed rozpoczęciem tego zadania należy się upewnić, że:

- Administrator sieci sprawdził, że połączenie jest dozwolone. Więcej informacji zawiera sekcja [“Przygotowanie do konfigurowania konsoli HMC” na stronie 49](#).
- Jeśli konfigurowana jest komunikacja przez Internet za pośrednictwem serwera proxy, potrzebne są dodatkowo następujące informacje:
 - adres IP i port serwera proxy,
 - dane uwierzytelniające serwera proxy.
- Używany jest adapter oznaczony jako **eth1** (wyznaczony do łączenia się z siecią otwartą). Więcej informacji zawiera sekcja [“Wybór ustawień sieciowych konsoli HMC” na stronie 40](#).
- Konsola HMC jest fizycznie podłączona do sieci LAN kablem ethernetowym.

Aby skonfigurować konsolę HMC jako serwer zgłoszeń automatycznych za pomocą kreatora konfiguracji zgłoszeń automatycznych, wykonaj następujące kroki:

Procedura

1. W obszarze nawigacyjnym kliknij ikonę **Serviceability** (Funkcje serwisowania) , a następnie wybierz opcję **Service Management** (Zarządzanie funkcjami serwisowymi).
2. W panelu zawartości kliknij opcję **Call-Home Setup Wizard** (Kreator konfiguracji zgłoszeń automatycznych). Zostanie otwarty kreator połączeń i serwerów zgłoszeń automatycznych. Postępuj zgodnie z instrukcjami kreatora, aby skonfigurować zgłoszenia automatyczne.

Konfigurowanie lokalnej konsoli w celu zgłaszania błędów do działu serwisu i wsparcia

W sekcji opisano konfigurowanie konsoli HMC w celu automatycznego zgłaszania błędów przez sieć LAN.

Konfigurowanie na konsoli HMC łączności z działem serwisu i wsparcia przy użyciu połączenia internetowego w sieci LAN i protokołu SSL

W sekcji opisano konfigurowanie konsoli HMC jako serwera zgłoszeń automatycznych z wykorzystaniem bezpośredniego (przez sieć LAN) i pośredniego (przez SSL) połączenia z Internetem.

Zanim rozpoczniesz

Przed rozpoczęciem tego zadania należy się upewnić, że:

- Administrator sieci sprawdził, że połączenie jest dozwolone. Więcej informacji zawiera sekcja [“Przygotowanie do konfigurowania konsoli HMC” na stronie 49](#).

- Zostały skonfigurowane informacje kontaktowe klienta. Aby sprawdzić informacje kontaktowe, należy przejść do interfejsu konsoli HMC i kliknąć opcję **Serviceability > Service Management > Manage Customer Information** (Funkcje serwisowania > Zarządzanie funkcjami serwisowymi > Zarządzanie informacjami o kliencie).
- Jeśli konfigurowana jest komunikacja przez Internet za pośrednictwem serwera proxy, potrzebne są dodatkowo następujące informacje:
 - adres IP i port serwera proxy,
 - dane uwierzytelniające serwera proxy.
- Musi być skonfigurowany co najmniej jeden interfejs sieci otwartej. Więcej informacji zawiera sekcja [“Sieci prywatne i otwarte w środowisku konsoli HMC” na stronie 42.](#)
- Konsola HMC jest fizycznie podłączona do sieci LAN kablem ethernetowym.

O tym zadaniu

Aby skonfigurować konsolę HMC jako serwer zgłoszeń automatycznych z użyciem komunikacji w sieci LAN przez Internet oraz protokołu SSL, wykonaj następujące kroki:

Procedura



1. W obszarze nawigacyjnym kliknij ikonę **Serviceability** (Funkcje serwisowania), a następnie wybierz opcję **Service Management** (Zarządzanie funkcjami serwisowymi).
2. W sekcji Connectivity (Połączenia) kliknij opcję **Manage Outbound Connectivity** (Zarządzanie łącznością wychodzącą). Zostanie otwarte okno Call-home Server Consoles (Konsole serwera zgłoszeń automatycznych).
3. Kliknij opcję **Configure** (Konfiguruj).
4. W oknie Outbound Connectivity Settings (Ustawienia połączeń wychodzących) zaznacz opcję **Enable the local console as a call-home server** (Aktywuj konsolę lokalną jako serwer zgłoszeń automatycznych).
5. Zaakceptuj umowę.
6. W oknie Outbound Connectivity Settings (Ustawienia połączeń wychodzących) wybierz stronę **Internet**.
7. Zaznacz pole **Allow an existing internet connection for service** (Zezwól na serwis przy użyciu istniejącego połączenia internetowego).
8. Jeśli używany jest serwer proxy SSL, zaznacz pole **Use SSL proxy** (Użyj serwera proxy SSL).
9. Jeśli używany jest serwer proxy SSL, wpisz adres i port serwera proxy. Informacje te można uzyskać od administratora sieci.
10. Jeśli zostało zaznaczone pole **Use SSL proxy** (Użyj serwera proxy SSL), a serwer proxy wymaga uwierzytelnienia z wykorzystaniem nazwy użytkownika i hasła, zaznacz pole **Authenticate with the SSL proxy** (Uwierzytelniaj za pomocą serwera proxy SSL). Wpisz identyfikator użytkownika i hasło. Identyfikator użytkownika i hasło można uzyskać od administratora sieci.
11. Wybierz odpowiednią wartość w polu **Protocol to Internet** (Protokół dla dostępu do Internetu).
12. Na stronie **Internet** kliknij przycisk **Test** (Testuj).
13. W oknie Test internet (Testowanie połączenia z Internetem) kliknij przycisk **Start** (Uruchom).
14. Sprawdź, czy test został zakończony pomyślnie.
15. W oknie Test internet (Testowanie połączenia z Internetem) kliknij przycisk **Cancel** (Anuluj).
16. W oknie Outbound Connectivity Settings (Ustawienia połączeń wychodzących) kliknij przycisk **OK**.

Wybór istniejących serwerów zgłoszeń automatycznych do nawiązywania połączeń z działem serwisu i wsparcia z bieżącej konsoli HMC

Sekcja zawiera informacje na temat wybierania istniejących serwerów zgłoszeń automatycznych konsoli HMC rozpoznanych lub wykrytych przez bieżącą konsolę w celu zgłaszania błędów.

Zanim rozpocznieasz

Wykryte konsole HMC to takie konsole, na których włączone są serwery zgłoszeń automatycznych i które znajdują się w tej samej podsieci lub zarządzają tym samym systemem zarządzanym, co bieżąca konsola HMC.

Aby wybrać wykrytą konsolę HMC, za pośrednictwem której będą automatycznie wysyłane zgłoszenia błędów, wykonaj następujące kroki:

Procedura



1. W obszarze nawigacyjnym kliknij ikonę **Serviceability** (Funkcje serwisowania), a następnie wybierz opcję **Service Management** (Zarządzanie funkcjami serwisowymi).
2. W panelu zawartości kliknij opcję **Manage Outbound Connectivity** (Zarządzanie łącznością wychodzącą). Zostanie otwarte okno Call-Home Server Consoles (Konsole serwera zgłoszeń automatycznych).
3. Kliknij opcję **Use discovered call-home server consoles** (Użyj wykrytych konsol serwera zgłoszeń automatycznych). Zostaną wyświetlone adresy IP lub nazwy hostów konsol HMC skonfigurowanych jako serwery zgłoszeń automatycznych.
4. Kliknij przycisk **OK**.

Wyniki

Można też ręcznie dodawać istniejące konsole HMC z serwerami zgłoszeń automatycznych, które znajdują się w innej podsieci. Należy wybrać adres IP lub nazwę hosta konsoli HMC, która jest skonfigurowana na potrzeby zgłoszeń automatycznych, i kliknąć przycisk **Add** (Dodaj), a następnie kliknąć przycisk **OK**.

Sprawdzanie poprawnego działania połączenia z działem serwisu i wsparcia

Testowanie zgłaszania problemów w celu sprawdzenia poprawnego działania połączenia z działem serwisu i wsparcia.

O tym zadaniu

Aby sprawdzić poprawność konfiguracji zgłoszeń automatycznych, wykonaj następujące kroki:

Procedura



1. W obszarze nawigacyjnym kliknij ikonę **Serviceability** (Funkcje serwisowania), a następnie wybierz opcję **Service Management** (Zarządzanie funkcjami serwisowymi).
2. W panelu zawartości kliknij opcję **Create Event** (Utwórz zdarzenie).
3. Wybierz opcję **Test Automatic Problem Reporting** (Testuj automatyczne zgłaszanie problemu) i wpisz komentarz.
4. Kliknij opcję **Request Service** (Zażądaj serwisu). Zaczekaj kilka minut, aby żądanie zostało wysłane.
5. W oknie Service Management (Zarządzanie funkcjami serwisowymi) wybierz opcję **Manage Events** (Zarządzaj zdarzeniami).
6. Wybierz opcję **All open problems** (Wszystkie otwarte problemy).
7. Sprawdź, czy do otwartego numeru problemu przypisane są zdarzenie i numer PMH.
8. Wybierz to zdarzenie i kliknij opcję **Close** (Zamknij).
9. W oknie **Close** (Zamknij) wpisz nazwisko i krótki komentarz.

Nadawanie użytkownikom uprawnień do przeglądania zgromadzonych danych o systemie

Aby użytkownicy mogli przeglądać dane dotyczące systemów, muszą mieć odpowiednie uprawnienia.

Zanim rozpoczniesz

Nadawanie użytkownikom uprawnień do przeglądania zgromadzonych danych o systemie wymaga uprzedniego uzyskania identyfikatora IBM. Więcej informacji na temat uzyskiwania identyfikatora IBM zawiera sekcja [“Arkusze konfiguracji wstępnej dla konsoli HMC”](#) na stronie 50.

O tym zadaniu

Aby nadać użytkownikom uprawnienia do przeglądania zgromadzonych danych o systemie, wykonaj następujące kroki:

Procedura



1. W obszarze nawigacyjnym kliknij ikonę **Serviceability** (Funkcje serwisowania), a następnie wybierz opcję **Service Management** (Zarządzanie funkcjami serwisowymi).
2. W panelu zawartości wybierz opcję **Authorize User** (Nadaj uprawnienia użytkownikowi).
3. Wprowadź swój identyfikator IBM.
4. Kliknij przycisk **OK**.

Przesyłanie informacji serwisowych

Informacje serwisowe mogą być przesyłane do dostawcy usług natychmiast lub można zaplanować wysyłanie ich okresowo.

Zanim rozpoczniesz

IBM oferuje możliwość personalizowania funkcji dostępnych przez interfejs WWW na podstawie informacji gromadzonych przez aplikację IBM Electronic Service Agent. Aby można było skorzystać z tych funkcji, należy najpierw zarejestrować się w serwisie WWW IBM Registration pod adresem <http://www.ibm.com/account/profile>. Informacje na temat nadawania użytkownikom uprawnień do używania danych aplikacji Electronic Service Agent na potrzeby personalizacji funkcji dostępnych przez interfejs WWW zawiera sekcja [“Nadawanie użytkownikom uprawnień do przeglądania zgromadzonych danych o systemie”](#) na stronie 75. Więcej informacji na temat korzyści, jakie niesie zarejestrowanie identyfikatora IBM dla używanych systemów, można znaleźć pod adresem <http://www.ibm.com/support/electronic>.

Uwaga: Informacje serwisowe należy wysłać dostawcy usług bezpośrednio po zainstalowaniu i skonfigurowaniu konsoli HMC.

O tym zadaniu

Aby przestać informację serwisowe, wykonaj następujące kroki:

Procedura



1. W obszarze nawigacyjnym kliknij ikonę **Serviceability** (Funkcje serwisowania), a następnie wybierz opcję **Service Management** (Zarządzanie funkcjami serwisowymi).
2. W panelu zawartości kliknij opcję **Transmit Service Information** (Przesyłanie informacji serwisowych).
3. Wykonaj czynności opisane w oknie **Transmit Service Information** (Przesyłanie informacji serwisowych), a następnie kliknij przycisk **OK**.

Konfigurowanie Menedżera zdarzeń dla zgłoszeń automatycznych

Sekcja zawiera informacje dotyczące sposobu konfigurowania zadania Menedżer zdarzeń dla zgłoszeń automatycznych. Dane przekazywane z konsoli HMC do firmy IBM za pomocą tego zadania można monitorować i zatwierdzać.

Tryb Menedżer zdarzeń dla zgłoszeń automatycznych (włączony lub wyłączony) jest ustawiany za pomocą interfejsu wiersza komend HMC. Włączenie zadania Menedżer zdarzeń dla zgłoszeń automatycznych

powoduje blokowanie na konsoli HMC zdarzeń zgłoszeń automatycznych, gdy takie wystąpią. Aby uniemożliwić zgłoszenie zdarzeń zgłaszanych automatycznie bez zatwierdzenia, wszystkie konsole HMC działające w tym środowisku muszą mieć włączone zadanie Menedżer zdarzeń dla zgłoszeń automatycznych.

Aby włączyć lub wyłączyć zadanie Menedżer zdarzeń dla zgłoszeń automatycznych, uruchom następującą komendę:

chhmc -c emch

-s {enable | disable}

[--callhome {enable | disable}]

[--help]

Uwaga: Włączenie zadania Menedżer zdarzeń dla zgłoszeń automatycznych powoduje wstrzymanie zdarzeń zgłoszeń automatycznych, dopóki nie zostaną one zatwierdzone dla zadania zgłoszeń automatycznych. Jeśli zadanie Menedżer zdarzeń dla zgłoszeń automatycznych zostanie wyłączone, to nie spowoduje to automatycznego włączenia opcji zgłoszeń automatycznych. Taka konfiguracja zapobiega nienadzorowanemu ponownemu zgłaszaniu automatycznemu danych do firmy IBM. Aby ustawić wymaganą konfigurację, wybierz spośród następujących opcji komendy:

- Aby włączyć zadanie Menedżer zdarzeń dla zgłoszeń automatycznych: **chhmc -c emch -s enable**
- Aby wyłączyć zadanie Menedżer zdarzeń dla zgłoszeń automatycznych i ponownie włączyć zgłoszenia automatyczne: **chhmc -c emch -s disable --callhome enable**
- Aby wyłączyć zadanie Menedżer zdarzeń dla zgłoszeń automatycznych i nie włączać ponownie zgłoszeń automatycznych: **chhmc -c emch -s disable --callhome disable**

Upewnij się, że konsola HMC może komunikować się z innymi konsolami HMC wdrożonymi w tym środowisku. Zadanie Menedżer zdarzeń dla zgłoszeń automatycznych ma funkcję testowania połączenia, jeśli konsola HMC jest zarejestrowana.

Konsolę HMC można zarejestrować za pomocą Menedżera zdarzeń dla zgłoszeń automatycznych. Po zarejestrowaniu konsoli HMC menedżer zdarzeń odpytuje zarejestrowaną konsolę HMC o zdarzenia oczekujące na zgłoszenie automatyczne do IBM. Menedżer zdarzeń przedstawia, jakie dane są wysyłane z powrotem do IBM, i zatwierdza te zdarzenia. Po zatwierdzeniu menedżer zdarzeń powiadamia zarejestrowaną konsolę HMC o możliwości kontynuowania operacji zgłoszenia automatycznego.

Zadanie Menedżer zdarzeń dla zgłoszeń automatycznych można uruchomić z dowolnej konsoli HMC lub z wielu konsol HMC. Aby zarejestrować konsolę zarządzania za pomocą zadania Menedżer zdarzeń dla zgłoszeń automatycznych, wykonaj następujące kroki:



1. W obszarze nawigacyjnym kliknij ikonę **Serviceability** (Funkcje serwisowania), a następnie wybierz opcję **Events Manager for Call Home** (Menedżer zdarzeń dla zgłoszeń automatycznych).
2. Na panelu **Events Manager for Call Home** (Menedżer zdarzeń dla zgłoszeń automatycznych) kliknij opcję **Manage Consoles** (Zarządzaj konsolami).
3. W oknie **Manage Registered Consoles** (Zarządzaj zarejestrowanymi konsolami) kliknij opcję **Add Console** (Dodaj konsolę), aby wprowadzić informacje w celu zarejestrowania konsoli zarządzania za pomocą zadania Menedżer zdarzeń dla zgłoszeń automatycznych.
4. Kliknij przycisk **OK**, aby zatwierdzić zmiany listy zarejestrowanych konsol zarządzania.

Uwaga: Zadanie Menedżer zdarzeń dla zgłoszeń automatycznych może być używane z wyłączonym trybem menedżera zdarzeń. Nadal możliwe jest zarejestrowanie konsoli HMC i wyświetlanie zdarzeń w menedżerze zdarzeń, ale menedżer zdarzeń nie steruje automatycznym zgłaszaniem zdarzeń.

Ustawianie haseł dla systemu zarządzanego

Konieczne jest ustawienie haseł zarówno dla serwera, jak i interfejsu ASMI. Sekcja zawiera informacje na temat ustawiania tych haseł za pomocą interfejsu konsoli HMC.

Zanim rozpocznieś

Jeśli został wyświetlony komunikat Authentication Pending (Uwierzytelnianie w toku), konsola HMC wyświetli zachętę do zdefiniowania haseł dla systemu zarządzanego.

O tym zadaniu

Jeśli komunikat Authentication Pending (Uwierzytelnianie w toku) nie został wyświetlony, należy wykonać wymienione niżej czynności, aby ustawić hasła dla systemu zarządzanego.

Aktualizowanie hasła serwera

Zanim rozpocznieś

Aby zaktualizować hasło serwera, wykonaj następujące kroki:

Procedura

1. W obszarze nawigacyjnym wybierz system zarządzany i kliknij ikonę **Users and Security** (Użytkownicy i



bezpieczeństwo), a następnie wybierz opcję **Users and Roles** (Użytkownicy i role).

2. Kliknij opcję **Change Password** (Zmiana hasła). Zostanie otwarte okno Update Password (Aktualizuj hasło).
3. Wpisz wymagane informacje i kliknij przycisk **OK**.

Aktualizowanie hasła ogólnego ASM

Zanim rozpocznieś

Uwaga: Domyślne hasło zwykłego użytkownika to `general`, a domyślne hasło administratora to `admin`.

Aby zaktualizować ogólne hasło interfejsu ASMI, wykonaj następujące kroki:

Procedura

1. W obszarze nawigacyjnym konsoli HMC wybierz system zarządzany.
2. W obszarze zadań kliknij opcję **Operations** (Operacje).
3. Kliknij opcję **Advanced System Management (ASM)** (Zaawansowane zarządzanie systemem (ASM)). Zostanie otwarte okno Launch ASM Interface (Uruchom interfejs ASM).
4. Wybierz adres IP procesora serwisowego i kliknij przycisk **OK**. Zostanie otwarty interfejs ASMI.
5. W panelu powitania interfejsu ASMI podaj identyfikator użytkownika i hasło, a następnie kliknij przycisk **Log In** (Zaloguj się).
6. W obszarze nawigacyjnym kliknij opcję **Login Profile** (Profil logowania).
7. Wybierz opcję **Change Password** (Zmiana hasła).
8. Podaj wymagane informacje, a następnie kliknij przycisk **Continue** (Kontynuuj).

Resetowanie hasła administratora zaawansowanego zarządzania systemem (ASM)

Zanim rozpocznieś

Aby zresetować hasło administratora, należy skontaktować się z autoryzowanym dostawcą usług.

Testowanie połączenia między konsolą HMC a systemem zarządzanym

Sekcja zawiera informacje na temat weryfikowania poprawności podłączenia do sieci.

O tym zadaniu

Testowanie połączeń sieciowych może być wykonywane przez użytkowników, którzy mają przypisaną jedną z następujących ról:

- Główny administrator
- Przedstawiciel serwisu

Aby przetestować połączenie między konsolą HMC a systemem zarządzanym, wykonaj następujące kroki:

Procedura

1. W obszarze nawigacyjnym kliknij ikonę **HMC Management** (Zarządzanie konsolą HMC)  , a następnie wybierz opcję **Console Settings** (Ustawienia konsoli).
2. W panelu zawartości kliknij opcję **Test Network Connectivity** (Testowanie połączeń sieciowych).
3. Na karcie Ping wpisz nazwę hosta lub adres IP systemu, z którym chcesz się połączyć. Aby przetestować sieć otwartą, wpisz adres bramy. Kliknij opcję **Ping**.

Wyniki

Jeśli nie zostały jeszcze utworzone żadne partycje logiczne, nie można wysłać pakietu ping pod te adresy. Za pomocą konsoli HMC można tworzyć partycje logiczne na serwerze. Więcej informacji zawiera sekcja [Partycjonowanie logiczne](#).

Aby poznać sposoby używania konsoli HMC w sieci, należy zapoznać się z sekcją [“Połączenia sieciowe konsoli HMC”](#) na stronie 40.

Więcej informacji na temat konfigurowania połączenia konsoli HMC z siecią zawiera sekcja [“Konfigurowanie konsoli HMC za pomocą menu ”](#) na stronie 58.

Czynności pokonfiguracyjne

Po zainstalowaniu i skonfigurowaniu konsoli HMC należy utworzyć niezbędne kopie zapasowe danych konsoli HMC.

Tworzenie kopii zapasowej danych konsoli zarządzania

Zadanie to pozwala utworzyć kopię zapasową (lub archiwalną) danych, które są przechowywane na dysku twardym konsoli HMC i mają niewrażliwe znaczenie dla jej działania.

Zanim rozpoczniesz

System zdalny musi mieć skonfigurowany system plików NFS (Network File System) lub połączenie Secure Shell (ssh), a sieć musi być dostępna z konsoli HMC. Aby wykonać to zadanie, należy wyłączyć i uruchomić ponownie konsolę HMC. Do wykonania tych czynności należy używać jedynie konsoli HMC.

O tym zadaniu

Aby utworzyć kopię zapasową napędu dysku twardego konsoli HMC w systemie zdalnym, użytkownik musi mieć przypisaną jedną z następujących ról:

- Główny administrator
- Operator
- Przedstawiciel serwisu

Kopie zapasowe danych konsoli HMC należy tworzyć po wprowadzeniu zmian w tej konsoli lub zmodyfikowaniu informacji związanych z partycjami logicznymi.

Dane konsoli HMC przechowywane na jej dysku twardym można zapisać na dysku DVD-RAM w systemie lokalnym lub w systemie zdalnym podłączonym do systemu plików konsoli HMC (np. NFS) bądź przesłać do zdalnego serwisu z wykorzystaniem protokołu FTP.

Uwaga: W przypadku konsoli HMC model 7063-CR1 można podłączyć zewnętrzny napęd DVD ze złączem USB.

Za pomocą konsoli HMC można utworzyć kopie zapasowe wszystkich najważniejszych danych, takich jak:

- pliki preferencji użytkowników
- informacje o użytkownikach
- pliki konfiguracji platformy konsoli HMC
- pliki dziennika konsoli HMC
- aktualizacje konsoli HMC poprzez instalację poprawek

Aby utworzyć kopię zapasową dysku twardego konsoli HMC w systemie zdalnym, wykonaj następujące kroki:

Procedura

1. W obszarze nawigacyjnym kliknij ikonę **HMC Management** (Zarządzanie konsolą HMC) , a następnie wybierz opcję **Console Management** (Zarządzanie konsolą).
2. W panelu zawartości kliknij opcję **Backup Management Console Data** (Tworzenie kopii zapasowej danych konsoli zarządzania).
3. W oknie **Backup Management Console Data** (Tworzenie kopii zapasowej danych konsoli zarządzania) wybierz opcję archiwizacji, którą chcesz wykonać.
4. Kliknij przycisk **Next** (Dalej), a następnie postępuj zgodnie z instrukcjami właściwymi dla wybranej opcji.
5. Kliknij przycisk **OK**, aby kontynuować proces tworzenia kopii zapasowej.

Aktualizowanie i migrowanie kodu maszynowego konsoli HMC

Okresowo udostępniane są aktualizacje konsoli HMC, mające na celu dodawanie nowych możliwości i ulepszanie istniejących funkcji. Rozdział zawiera informacje na temat różnic między aktualizowaniem, aktualizowaniem do nowej wersji i migrowaniem kodu maszynowego konsoli HMC. Opisano tu również, w jaki sposób aktualizować i migrować kod maszynowy konsoli HMC.

Po zakończeniu wszystkich tych czynności konsola HMC zostanie uruchomiona ponownie, ale nie zostaną ponownie uruchomione partycje.

Aktualizowanie kodu konsoli HMC

Instalowanie poprawek i aktualizacji istniejącego poziomu konsoli HMC

Nie wymaga wykonywania czynności **Save upgrade data** (Zapisywanie danych aktualizacji)

Aktualizowanie kodu konsoli HMC do nowej wersji

Wymiana oprogramowania konsoli HMC na nową wersję lub nowy poziom poprawek tego samego programu

Wymaga uruchomienia systemu z nośników odzyskiwania

Migrowanie kodu konsoli HMC

Przeniesienie danych konsoli HMC z jednej wersji konsoli HMC na inną

Migracja jest typem aktualizacji.

Uwaga: W przypadku konsoli HMC model 7063-CR1 można podłączyć zewnętrzny napęd DVD ze złączem USB.

Określanie wersji i wydania kodu maszynowego konsoli HMC

Sekcja zawiera informacje na temat określania wersji i wydania kodu maszynowego konsoli HMC.

O tym zadaniu

Wersja kodu maszynowego konsoli HMC ma wpływ na dostępne opcje, takie jak obsługa oprogramowania wbudowanego serwera w trakcie pracy systemu i rozszerzenia aktualizacji do nowego wydania.

Aby wyświetlić wersję i wydanie kodu maszynowego konsoli HMC, wykonaj następujące kroki:

Procedura

1. W obszarze nawigacyjnym kliknij ikonę **HMC Management** (Zarządzanie konsolą HMC) , a następnie wybierz opcję **Console Management** (Zarządzanie konsolą).
2. W panelu zawartości kliknij opcję **Update the Hardware Management Console** (Aktualizacja konsoli HMC).
3. W nowym oknie przejrzyj i zapisz informacje widoczne poniżej nagłówka **Current HMC Driver Information** (Bieżące informacje o sterowniku konsoli HMC), w tym: wersję, wydanie, poziom poprawek, wersję kompilacji i wersje podstawowe konsoli HMC.

Uzyskiwanie i stosowanie aktualizacji kodu maszynowego konsoli HMC dysponującej połączeniem z Internetem

Sekcja zawiera informacje na temat uzyskiwania aktualizacji kodu maszynowego konsoli HMC, gdy konsola ma połączenie internetowe.

O tym zadaniu

Aby uzyskać aktualizację kodu maszynowego konsoli HMC, wykonaj wszystkie kroki.

Krok 1. Upewnij się, że dysponujesz połączeniem internetowym

O tym zadaniu

Aby było możliwe pobranie aktualizacji z serwisu WWW lub systemu serwisu i wsparcia na konsolę HMC lub serwer, musi być dostępne jedno z następujących połączeń:

- Połączenie SSL z użyciem serwera proxy SSL lub bez niego
- Internet VPN (Internetowa sieć VPN)

Aby upewnić się, że dysponujesz połączeniem internetowym, wykonaj następujące czynności:

Procedura

1. W obszarze nawigacyjnym kliknij ikonę **Serviceability** (Funkcje serwisowania) , a następnie wybierz opcję **Service Management** (Zarządzanie funkcjami serwisowymi).
2. W panelu zawartości kliknij opcję **Manage Outbound Connectivity** (Zarządzanie łącznością wychodzącą).
3. Wybierz kartę odpowiednią dla typu połączeń wychodzących wybranego dla konsoli HMC: Internet VPN (Internetowa sieć VPN) lub SSL connectivity (Połączenie przez SSL).

Uwaga: Jeśli nie ma połączenia z serwisem i wsparciem, należy ustawić połączenie serwisowe z wykorzystaniem tej procedury. Instrukcje dotyczące konfigurowania połączenia z serwisem i wsparciem zawiera sekcja Konfigurowanie serwera do połączenia z serwisem i wsparciem IBM.

4. Kliknij przycisk **Test** (Testuj).
5. Sprawdź, czy test został zakończony pomyślnie.
Jeśli test nie został zakończony pomyślnie, należy znaleźć błąd w połączeniu i usunąć problem przed przystąpieniem do wykonywania procedury. Inną możliwością jest zaopatrzenie się w aktualizację na dysku DVD.
Uwaga: W przypadku konsoli HMC model 7063-CR1 można podłączyć zewnętrzny napęd DVD ze złączem USB.
6. Przejdź do sekcji [“Krok 2. Wyświetl aktualną wersję kodu maszynowego konsoli HMC” na stronie 82.](#)

Krok 2. Wyświetl aktualną wersję kodu maszynowego konsoli HMC

O tym zadaniu

Aby wyświetlić aktualną wersję kodu maszynowego konsoli HMC, wykonaj następujące kroki:

Procedura

1. W obszarze nawigacyjnym kliknij ikonę **HMC Management** (Zarządzanie konsolą HMC) , a następnie wybierz opcję **Console Management** (Zarządzanie konsolą).
2. W panelu zawartości kliknij opcję **Update the Hardware Management Console** (Aktualizacja konsoli HMC).
3. W nowym oknie przejrzyj i zapisz informacje widoczne poniżej nagłówka Current HMC Driver Information (Bieżące informacje o sterowniku konsoli HMC), w tym: wersję, wydanie, poziom poprawek, wersję kompilacji i wersję podstawowe konsoli HMC.
4. Przejdź do sekcji [“Krok 3. Zapoznaj się z dostępnymi wersjami kodu maszynowego konsoli HMC” na stronie 82.](#)

Krok 3. Zapoznaj się z dostępnymi wersjami kodu maszynowego konsoli HMC

O tym zadaniu

Aby wyświetlić dostępne wersje kodu maszynowego konsoli HMC, wykonaj następujące kroki:

Procedura

1. Na komputerze lub serwerze mającym połączenie internetowe otwórz serwis WWW <http://www.ibm.com/eserver/support/fixes>.
2. Zaznacz odpowiednią rodzinę na liście Product family (Rodzina produktów).
3. Na liście Product or fix type (Produkt lub typ poprawki) zaznacz pozycję **Hardware Management Console** (Konsola HMC).
4. Kliknij przycisk **Continue** (Kontynuuj).
Zostanie wyświetlona strona Hardware Management Console (Konsola HMC).
5. Przewiń stronę do posiadanego poziomu wersji konsoli HMC, aby przejrzeć dostępne poziomy konsoli HMC.
Uwaga: Można także skontaktować się z serwisem i wsparciem.
6. Przejdź do sekcji [“Krok 4. Zainstaluj aktualizację kodu maszynowego konsoli HMC” na stronie 82.](#)

Krok 4. Zainstaluj aktualizację kodu maszynowego konsoli HMC

O tym zadaniu

Aby zastosować aktualizację kodu maszynowego konsoli HMC, wykonaj następujące kroki:

Procedura

1. Przed rozpoczęciem instalowania aktualizacji kodu maszynowego konsoli HMC utwórz kopię zapasową niewrażliwych danych przechowywanych na konsoli HMC.
Odpowiednie instrukcje zawiera sekcja [“Tworzenie kopii zapasowej danych konsoli zarządzania”](#) na stronie 79. Następnie kontynuuj działania.



2. W obszarze nawigacyjnym kliknij ikonę **HMC Management** (Zarządzanie konsolą HMC), a następnie wybierz opcję **Console Management** (Zarządzanie konsolą).
3. W panelu zawartości kliknij opcję **Update the Hardware Management Console** (Aktualizacja konsoli HMC). Zostanie otwarty kreator Install Corrective Service (Instaluj poprawkę).
4. Postępuj zgodnie z instrukcjami kreatora, aby zainstalować aktualizację.
5. Wyłącz i uruchom ponownie konsolę HMC, aby aktualizacja została zastosowana.
6. Kliknij opcję **Log on and launch the Hardware Management Console web application** (Zaloguj się i uruchom aplikację WWW konsoli HMC).
7. Zaloguj się w interfejsie konsoli HMC.

Krok 5. Sprawdź, czy aktualizacja kodu maszynowego konsoli HMC została zainstalowana pomyślnie

O tym zadaniu

Aby sprawdzić, czy aktualizacja kodu maszynowego konsoli HMC została poprawnie zainstalowana, wykonaj następujące kroki:

Procedura



1. W obszarze nawigacyjnym kliknij ikonę **HMC Management** (Zarządzanie konsolą HMC), a następnie wybierz opcję **Console Management** (Zarządzanie konsolą).
2. W panelu zawartości kliknij opcję **Update the Hardware Management Console** (Aktualizacja konsoli HMC).
3. W nowym oknie przejrzyj i zapisz informacje widoczne poniżej nagłówka Current HMC Driver Information (Bieżące informacje o sterowniku konsoli HMC), w tym: wersję, wydanie, poziom poprawek, wersję kompilacji i wersje podstawowe konsoli HMC.
4. Upewnij się, że wersja i wydanie odpowiadają instalowanej aktualizacji.
5. Jeśli poziom oprogramowania wbudowanego nie odpowiada zainstalowanej aktualizacji, wykonaj następujące czynności:
 - a. Wybierz połączenie sieciowe konsoli HMC.
 - b. Ponów aktualizację oprogramowania wbudowanego przy użyciu innego repozytorium.
 - c. Jeśli problem wystąpi ponownie, skontaktuj się ze wsparciem wyższego poziomu.

Uzyskiwanie i stosowanie aktualizacji kodu maszynowego konsoli HMC z wykorzystaniem dysku DVD lub serwera FTP

Sekcja zawiera informacje na temat uzyskiwania aktualizacji kodu maszynowego konsoli HMC (Hardware Management Console) przy użyciu dysku DVD lub serwera FTP.

O tym zadaniu

Aby uzyskać aktualizację kodu maszynowego konsoli HMC, należy wykonać wszystkie kroki.

Uwaga: W przypadku konsoli HMC model 7063-CR1 można podłączyć zewnętrzny napęd DVD ze złączem USB.

Krok 1. Wyświetl aktualną wersję kodu maszynowego konsoli HMC

Zanim rozpoczniesz

Aby wyświetlić aktualną wersję kodu maszynowego konsoli HMC, wykonaj następujące kroki:

Procedura

1. W obszarze nawigacyjnym kliknij ikonę **HMC Management** (Zarządzanie konsolą HMC) , a następnie wybierz opcję **Console Management** (Zarządzanie konsolą).
2. W panelu zawartości kliknij opcję **Update the Hardware Management Console** (Aktualizacja konsoli HMC).
3. W nowym oknie przejrzyj i zapisz informacje widoczne poniżej nagłówka Current HMC Driver Information (Bieżące informacje o sterowniku konsoli HMC), w tym: wersję, wydanie, poziom poprawek, wersję kompilacji i wersje podstawowe konsoli HMC.
4. Przejdź do sekcji [“Krok 2. Zapoznaj się z dostępnymi wersjami kodu maszynowego konsoli HMC” na stronie 84.](#)

Krok 2. Zapoznaj się z dostępnymi wersjami kodu maszynowego konsoli HMC

Zanim rozpoczniesz

Aby wyświetlić dostępne wersje kodu maszynowego konsoli HMC, wykonaj następujące kroki:

O tym zadaniu

Procedura

1. Na komputerze lub serwerze z połączeniem internetowym przejdź do serwisu [WWW Fix Central](#).
 2. Przewiń stronę do posiadanego poziomu wersji konsoli HMC, aby przejrzeć dostępne poziomy konsoli HMC.
- Uwaga:** Możesz także skontaktować się z działem serwisu i wsparcia IBM.
3. Przejdź do sekcji [“Krok 3. Uzyskaj aktualizację kodu maszynowego konsoli HMC” na stronie 84.](#)

Krok 3. Uzyskaj aktualizację kodu maszynowego konsoli HMC

Zanim rozpoczniesz

Aby uzyskać aktualizację kodu maszynowego konsoli HMC, wykonaj następujące kroki:

O tym zadaniu

Aktualizację kodu maszynowego konsoli HMC możesz zamówić w serwisie [WWW Fix Central](#) lub pobrać na serwer FTP; możesz się także skontaktować z działem serwisu i wsparcia.

Zamawianie aktualizacji kodu maszynowego konsoli HMC za pośrednictwem serwisu WWW Fix Central

1. Na komputerze lub serwerze z połączeniem internetowym przejdź do serwisu [WWW Fix Central](#).
2. W sekcji Supported HMC products (Obsługiwane produkty HMC) wybierz najnowszy poziom konsoli HMC.

3. Przewiń w dół do obszaru nazw plików / pakietu i odszukaj aktualizację, która ma zostać zamówiona.
4. W kolumnie Order (Zamów) wybierz opcję **Go** (Wykonaj).
5. Kliknij przycisk **Continue** (Kontynuuj), aby zalogować się za pomocą swojego identyfikatora IBM.
6. Postępuj zgodnie ze wskazówkami na ekranie, aby wystać zamówienie.

Pobieranie aktualizacji kodu maszynowego konsoli HMC na nośnik wymienny

1. Na komputerze lub serwerze z połączeniem internetowym przejdź do serwisu [WWW Fix Central](#).
2. W sekcji Supported HMC products (Obsługiwane produkty HMC) wybierz najnowszy poziom konsoli HMC.
3. Przewiń w dół do obszaru nazw plików / pakietu i odszukaj aktualizację, którą chcesz pobrać.
4. Kliknij aktualizację, którą chcesz pobrać.
5. Zaakceptuj warunki licencji i zapisz aktualizację na nośniku wymiennym.

Co dalej

Po zakończeniu tego etapu przejdź do sekcji [“Krok 4. Zainstaluj aktualizację kodu maszynowego konsoli HMC”](#) na stronie 85.

Krok 4. Zainstaluj aktualizację kodu maszynowego konsoli HMC

Zanim rozpoczniesz

Aby zastosować aktualizację kodu maszynowego konsoli HMC, wykonaj następujące kroki:

Procedura

1. Przed rozpoczęciem instalowania aktualizacji kodu maszynowego konsoli HMC utwórz kopię zapasową danych konsoli HMC. Więcej informacji na ten temat zawiera sekcja [“Tworzenie kopii zapasowej danych konsoli zarządzania”](#) na stronie 79.
2. Jeśli aktualizacja została zamówiona lub zapisana na dysku DVD-RAM, włóż dysk do napędu DVD konsoli HMC. Jeśli aktualizacja została zamówiona lub zapisana na urządzeniu pamięci USB, włóż urządzenie pamięci do odpowiedniego gniazda.
3. Przed rozpoczęciem instalowania aktualizacji kodu maszynowego konsoli HMC utwórz kopię zapasową niewrażliwych danych przechowywanych na konsoli HMC.
Odpowiednie instrukcje zawiera sekcja [“Tworzenie kopii zapasowej danych konsoli zarządzania”](#) na stronie 79. Następnie kontynuuj działania.



4. W obszarze nawigacyjnym kliknij ikonę **HMC Management** (Zarządzanie konsolą HMC), a następnie wybierz opcję **Console Management** (Zarządzanie konsolą).
5. W panelu zawartości kliknij opcję **Update the Hardware Management Console** (Aktualizacja konsoli HMC). Zostanie otwarty kreator Install Corrective Service (Instaluj poprawkę).
6. Postępuj zgodnie z instrukcjami kreatora, aby zainstalować aktualizację.
7. Aby aktualizacja została zastosowana, wyłącz i zrestartuj konsolę HMC, a następnie ponownie się do niej zaloguj.
8. Przejdź do sekcji [“Krok 5. Sprawdź, czy aktualizacja kodu maszynowego konsoli HMC została zainstalowana pomyślnie”](#) na stronie 86.

Krok 5. Sprawdź, czy aktualizacja kodu maszynowego konsoli HMC została zainstalowana pomyślnie

Zanim rozpoczniesz

Aby sprawdzić, czy aktualizacja kodu maszynowego konsoli HMC została pomyślnie zainstalowana, wykonaj następujące kroki:

Procedura



1. W obszarze nawigacyjnym kliknij ikonę **HMC Management** (Zarządzanie konsolą HMC), a następnie wybierz opcję **Console Management** (Zarządzanie konsolą).
2. W panelu zawartości kliknij opcję **Update the Hardware Management Console** (Aktualizacja konsoli HMC).
3. W nowym oknie przejrzyj i zapisz informacje widoczne poniżej nagłówka Current HMC Driver Information (Bieżące informacje o sterowniku konsoli HMC), w tym: wersję, wydanie, poziom poprawek, wersję kompilacji i wersje podstawowe konsoli HMC.
4. Upewnij się, że wersja i wydanie odpowiadają instalowanej aktualizacji.
5. Jeśli wyświetlona wersja kodu nie odpowiada zainstalowanej aktualizacji, wykonaj następujące kroki:
 - a. Ponów próbę aktualizacji kodu maszynowego. Jeśli utworzono dysk DVD dla tej procedury, użyj nowego nośnika.
 - b. Jeśli problem wystąpi ponownie, skontaktuj się ze wsparciem wyższego poziomu.

Aktualizowanie oprogramowania konsoli HMC do nowej wersji

Sekcja zawiera informacje na temat aktualizowania oprogramowania konsoli HMC z jednej wersji do kolejnej przy zachowaniu istniejących danych konfiguracyjnych konsoli HMC.

O tym zadaniu

Aby zaktualizować kod maszynowy konsoli HMC, należy wykonać wszystkie kroki.

Uwaga: W przypadku konsoli HMC 7063-CR1 i 7063-CR2 można podłączyć zewnętrzny napęd DVD ze złączem USB.

Krok 1. Uzyskaj aktualizację

O tym zadaniu

Aktualizację kodu maszynowego konsoli HMC można zamówić w serwisie [WWW Fix Central](http://www.ibm.com/support/fixcentral/).

Aby uzyskać aktualizację za pośrednictwem serwisu [WWW Fix Central](http://www.ibm.com/support/fixcentral/), wykonaj następujące kroki:

Procedura

1. Na komputerze lub serwerze mającym połączenie internetowe otwórz serwis WWW konsoli HMC pod adresem <http://www-933.ibm.com/support/fixcentral/>.
2. Kliknij przycisk **Continue** (Kontynuuj).
Zostanie wyświetlona strona Hardware Management Console (Konsola HMC).
3. Przejdź do docelowej wersji konsoli HMC.
4. Odszukaj sekcję pobierania i zamawiania.
Uwaga: W przypadku braku dostępu do Internetu skontaktuj się z serwisem i wsparciem IBM, aby zamówić aktualizację na dysku DVD.
5. Postępuj zgodnie ze wskazówkami na ekranie, aby wystąpić zamówienie.

6. Po uzyskaniu aktualizacji przejdź do sekcji [“Krok 2. Wyświetl aktualną wersję kodu maszynowego konsoli HMC”](#) na stronie 87.

Krok 2. Wyświetl aktualną wersję kodu maszynowego konsoli HMC

O tym zadaniu

Aby określić aktualną wersję kodu maszynowego konsoli HMC, wykonaj następujące czynności:

Procedura

1. W obszarze nawigacyjnym kliknij ikonę **HMC Management** (Zarządzanie konsolą HMC) , a następnie wybierz opcję **Console Management** (Zarządzanie konsolą). W obszarze nawigacyjnym kliknij opcję **Updates** (Aktualizacje).
2. W panelu zawartości kliknij opcję **Update the Hardware Management Console** (Aktualizacja konsoli HMC).
3. W nowym oknie przejrzyj i zapisz informacje widoczne poniżej nagłówka Current HMC Driver information (Bieżące informacje o sterowniku konsoli HMC), w tym: wersję, wydanie, poziom poprawek, wersję kompilacji i wersje podstawowe konsoli HMC.
4. Wykonaj czynności opisane w sekcji [“Krok 3. Utwórz kopię zapasową danych profilu systemu zarządzanego”](#) na stronie 87.

Krok 3. Utwórz kopię zapasową danych profilu systemu zarządzanego

O tym zadaniu

Aby utworzyć kopię zapasową danych profilu systemu zarządzanego, wykonaj następujące kroki:

Procedura

1. Wybierz system, którego dane profilu chcesz zapisać.
2. Wybierz kolejno opcje **Actions > View All Actions > Legacy > Manage Partition Data > Backup** (Działania > Wyświetl wszystkie działania > Wcześniejsze > Zarządzaj danymi partycji > Utwórz kopię zapasową).
3. Wpisz nazwę pliku kopii zapasowej i zapisz te informacje.
4. Kliknij przycisk **OK**.
5. Powtórz te kroki dla każdego systemu.
6. Wykonaj czynności opisane w sekcji [“Krok 4. Utwórz kopię zapasową danych konsoli HMC”](#) na stronie 87.

Krok 4. Utwórz kopię zapasową danych konsoli HMC

O tym zadaniu

Przed zainstalowaniem nowej wersji oprogramowania konsoli HMC należy utworzyć kopię zapasową danych konsoli, aby w razie wystąpienia problemów podczas aktualizacji oprogramowania było możliwe odtworzenie poprzedniego poziomu. Newralgicznych danych konsoli nie należy używać po pomyślnej aktualizacji do nowej wersji oprogramowania konsoli HMC.

Uwaga: Aby można było utworzyć kopię zapasową na nośniku wymiennym, nośnik ten musi być dostępny.

Aby utworzyć kopię zapasową danych konsoli HMC, wykonaj następujące kroki:

Procedura

1. Jeśli planowane jest tworzenie kopii zapasowej na nośniku, należy wykonać następujące czynności w celu sformatowania nośnika:

- a. Umieść nośnik w napędzie.

- b. W obszarze nawigacyjnym kliknij ikonę **Serviceability** (Funkcje serwisowania) , a następnie wybierz opcję **Service Management** (Zarządzanie funkcjami serwisowymi).

- c. W panelu zawartości kliknij opcję **Format Media** (Formatowanie nośnika).

- d. Wybierz typ nośnika.

- e. Wybierz typ formatu.

- f. Kliknij przycisk **OK**.

2. W obszarze nawigacyjnym kliknij ikonę **HMC Management** (Zarządzanie konsolą HMC) , a następnie wybierz opcję **Console Management** (Zarządzanie konsolą).

3. W panelu zawartości kliknij opcję **Backup Management Console Data** (Tworzenie kopii zapasowej danych konsoli zarządzania).

Zostanie wyświetlone okno **Backup Management Console Data** (Tworzenie kopii zapasowej danych konsoli zarządzania).

4. Wybierz opcję tworzenia archiwum.

Kopię zapasową danych można zapisać w systemie lokalnym lub w systemie zdalnym podłączonym do systemu plików konsoli HMC (na przykład NFS) bądź wysłać do zdalnego serwisu za pomocą protokołu FTP.

- Aby zapisać kopię zapasową danych w systemie lokalnym, wybierz opcję **Back up to media on local system** (Utwórz kopię zapasową w systemie lokalnym) i postępuj zgodnie z instrukcjami.
- Aby zapisać kopię zapasową danych w podłączonym systemie zdalnym, wybierz opcję **Back up to mounted remote system** (Utwórz kopię zapasową w podłączonym systemie zdalnym) i postępuj zgodnie z instrukcjami.
- Aby zapisać kopię zapasową danych w zdalnym serwisie FTP, wybierz opcję **Send back up critical data to remote site** (Wyślij kopię zapasową newralgicznych danych do zdalnego serwisu) i postępuj zgodnie z instrukcjami.

5. Wykonaj czynności opisane w sekcji [“Krok 5. Zapisz aktualne dane konfiguracyjne konsoli HMC”](#) na stronie 88.

Krok 5. Zapisz aktualne dane konfiguracyjne konsoli HMC

O tym zadaniu

Przed aktualizacją oprogramowania konsoli do nowej wersji należy zapisać dane konfiguracyjne konsoli w celu zachowania bezpieczeństwa.

Aby zapisać bieżącą konfigurację konsoli HMC, wykonaj następujące kroki:

Procedura

1. Wybierz system zarządzany lub dowolne partycje, dla których mają zostać zarejestrowane informacje konfiguracyjne konsoli HMC.
2. W menu kontekstowym wybierz opcję **Actions > Schedule Operations** (Działania > Planowanie operacji).
Zostaną wyświetlone wszystkie zaplanowane operacje dla wybranego obiektu.
3. Wybierz opcję **Sort > By Object** (Sortowanie > Według obiektu).

4. Zaznacz każdy obiekt i zapisz następujące informacje:

- Nazwa obiektu
- Data w harmonogramie
- Czas operacji (podany w formacie 24-godzinnym)
- Czy operacja jest powtarzana regularnie? Jeśli parametr Repetitive ma wartość Yes (Tak), wykonaj następujące kroki:
 - a. Wybierz kolejno opcje **View > Schedule Details** (Widok > Szczegóły harmonogramu).
 - b. Zapisz informacje o interwale.
 - c. Zamknij okno zaplanowanych operacji.
 - d. Powtórz czynności dla każdej zaplanowanej operacji.

5. Zamknij okno **Customize Scheduled Operations** (Dostosowywanie zaplanowanych operacji).

6. Wykonaj czynności opisane w sekcji [“Krok 6. Zapisz status komend zdalnych”](#) na stronie 89.

Krok 6. Zapisz status komend zdalnych

O tym zadaniu

Aby zapisać status komend zdalnych, wykonaj następujące kroki:

Procedura

1. W obszarze nawigacyjnym kliknij ikonę **Users and Security** (Użytkownicy i bezpieczeństwo) , a następnie wybierz opcję **Systems and Console Security** (Bezpieczeństwo systemów i konsoli).
2. W panelu zawartości kliknij opcję **Enable Remote Command Execution** (Włączanie zdalnego wykonywania komend).
3. Sprawdź, czy zaznaczone jest pole wyboru **Enable remote command execution using the ssh facility** (Włącz wykonywanie zdalnych komend przy użyciu komendy ssh).
4. Kliknij przycisk **Cancel** (Anuluj).
5. Wykonaj czynności opisane w sekcji [“Krok 7. Zapisz dane aktualizacji”](#) na stronie 89.

Krok 7. Zapisz dane aktualizacji

O tym zadaniu

Bieżącą konfigurację konsoli HMC można zapisać na wyznaczonej partycji dysku konsoli HMC lub na nośniku lokalnym. Dane aktualizacji należy zapisywać dopiero bezpośrednio przed zaktualizowaniem oprogramowania konsoli HMC do nowego wydania. Po aktualizacji można odtworzyć ustawienia konfiguracyjne konsoli HMC.

Uwaga: Dozwolony jest tylko jeden poziom kopii zapasowej danych. Za każdym razem, kiedy zapisywane są dane aktualizacji, wcześniejszy poziom jest zastępowany.

Aby zapisać dane aktualizacji, wykonaj następujące kroki:

Procedura

1. W obszarze nawigacyjnym kliknij ikonę **HMC Management** (Zarządzanie konsolą HMC) , a następnie wybierz opcję **Console Management** (Zarządzanie konsolą).
2. W panelu zawartości kliknij opcję **Save Upgrade Data** (Zapisywanie danych aktualizacji). Zostanie otwarty kreator **Save Upgrade Data** (Zapisywanie danych aktualizacji).

3. Wybierz nośnik, na którym chcesz zapisać dane aktualizacji. Po wybraniu opcji zapisania na nośniku wymiennym umieść nośnik w napędzie. Kliknij przycisk **Next** (Dalej).
4. Kliknij przycisk **Finish** (Zakończ).
5. Poczekaj na zakończenie zadania.
Jeśli zadanie zapisywania danych aktualizacji nie powiedzie się, przed podjęciem dalszych działań skontaktuj się ze wsparciem wyższego poziomu.
Uwaga: Jeśli zadanie zapisywania danych aktualizacji nie powiedzie się, nie należy kontynuować procesu aktualizacji.
6. Kliknij przycisk **OK**.
7. Wykonaj czynności opisane w sekcji [“Krok 8. Zaktualizuj oprogramowanie konsoli HMC”](#) na stronie 90.

Krok 8. Zaktualizuj oprogramowanie konsoli HMC

O tym zadaniu

Aby zaktualizować oprogramowanie konsoli HMC, zrestartuj system z nośnikiem wymiennym umieszczonym w napędzie DVD.

Procedura

1. Umieść nośnik HMC Product Installation w napędzie DVD.
2. W obszarze nawigacyjnym kliknij ikonę **HMC Management** (Zarządzanie konsolą HMC) , a następnie wybierz opcję **Console Management** (Zarządzanie konsolą).
3. W panelu zawartości wybierz opcję **Shutdown or Restart the Management Console** (Zamknij lub uruchom ponownie konsolę zarządzania).
4. Upewnij się, że zaznaczona jest opcja **Restart the HMC** (Zrestartuj konsolę HMC).
5. Kliknij przycisk **OK**.
Konsola HMC zostanie ponownie uruchomiona, a informacje o systemie zostaną przewinięte w oknie.
6. Wybierz **Upgrade** (Aktualizacja) i kliknij przycisk **Next** (Dalej).
7. Wybierz jedną z następujących opcji:
 - Jeśli dane aktualizacji zostały zapisane podczas poprzedniego zadania, przejdź do kolejnego kroku.
 - Jeśli dane aktualizacji nie zostały zapisane wcześniej podczas wykonywania procedury, konieczne jest ich zapisanie przed podjęciem kolejnych działań.
8. Wybierz opcję **Upgrade from media** (Aktualizacja z nośnika) i kliknij **Next** (Dalej).
9. Potwierdź ustawienia i kliknij przycisk **Finish** (Zakończ).
10. Postępuj zgodnie z instrukcjami.
Uwaga:
 - Jeśli wyświetlony zostanie pusty ekran, naciśnij spację, aby wyświetlić informacje.
 - Instalacja pierwszego dysku DVD może zająć około 20 minut.
11. Zaloguj się, używając swojego identyfikatora użytkownika i hasła.
Instalacja kodu konsoli HMC została zakończona.
12. Wykonaj czynności opisane w sekcji [“Krok 9. Sprawdź, czy aktualizacja kodu maszynowego konsoli HMC została zainstalowana pomyślnie”](#) na stronie 91.

Krok 9. Sprawdź, czy aktualizacja kodu maszynowego konsoli HMC została zainstalowana pomyślnie

O tym zadaniu

Aby sprawdzić, czy aktualizacja konsoli HMC została pomyślnie zainstalowana, wykonaj następujące kroki:

Procedura

1. W obszarze nawigacyjnym kliknij ikonę **HMC Management** (Zarządzanie konsolą HMC) , a następnie wybierz opcję **Console Management** (Zarządzanie konsolą).
2. W panelu zawartości kliknij opcję **Update the Hardware Management Console** (Aktualizacja konsoli HMC).
3. W nowym oknie przejrzyj i zapisz informacje widoczne poniżej nagłówka Current HMC Driver information (Bieżące informacje o sterowniku konsoli HMC), w tym: wersję, wydanie, poziom poprawek, wersję kompilacji i wersje podstawowe konsoli HMC.
4. Upewnij się, że wersja i wydanie odpowiadają instalowanej aktualizacji.
5. Jeśli wyświetlona wersja kodu nie odpowiada zainstalowanej wersji, ponów próbę aktualizacji przy użyciu nowego dysku DVD. Jeśli problem wystąpi ponownie, skontaktuj się ze wsparciem wyższego poziomu.

Zdalna aktualizacja konsoli HMC przy użyciu sieciowych obrazów aktualizacji

Sekcja zawiera informacje na temat aktualizowania oprogramowania konsoli HMC z miejsca zdalnego przy użyciu sieciowych obrazów aktualizacji.

O tym zadaniu

Sekcja zawiera informacje na temat aktualizowania oprogramowania konsoli HMC z miejsca zdalnego przy użyciu sieciowych obrazów aktualizacji.

Procedura

1. Na komputerze lub serwerze mającym połączenie z Internetem przejdź do serwisu WWW Hardware Management Console Support and downloads (<http://www14.software.ibm.com/webapp/set2/sas/f/hmcl/home.html>).
2. Pobierz odpowiednie obrazy sieciowe oprogramowania konsoli HMC w wersji 9 i zapisz je na serwerze FTP.
Plików tych nie można pobrać bezpośrednio do konsoli HMC. Należy je pobrać na serwer, który akceptuje żądania FTP.
3. Upewnij się, że zostały pobrane następujące pliki:
 - img2a
 - img3a
 - base.img
 - disk1.img
 - hmcnetworkfiles.sum
4. Zapisz dane aktualizacji na konsoli HMC. Uruchom następujące komendy, aby zapisać dane aktualizacji:
 - Aby zapisać dane zarówno na dysku DVD, jak i na dysku twardym, uruchom następujące komendy:
mount /media/cdrom
saveupgdata -r diskdvd

- Aby zapisać dane na dysku twardym, uruchom następującą komendę:
saveupgdata -r disk
5. Skopiuj pliki aktualizacji na startową partycję dyskową na konsoli HMC. Uruchom komendę **getupgfiles**, aby skopiować pliki.
Przykład: **getupgfiles -h <serwer FTP> -u <ID użytkownika> -d <katalog zdalny>** gdzie:
 - **serwer FTP** to nazwa hosta lub adres IP serwera FTP, na który zostały pobrane obrazy sieciowe oprogramowania konsoli HMC;
 - **ID użytkownika** to poprawny identyfikator użytkownika na serwerze FTP; jeśli hasło nie zostanie podane za pomocą argumentu **--passwd**, zostanie wyświetlone zapytanie o hasło;
 - **katalog zdalny** to katalog na serwerze FTP, w którym są zapisywane obrazy sieciowe oprogramowania konsoli HMC.
 6. Zrestartuj konsolę HMC, aby zaktualizować kod skopiowany na startową partycję dyskową. W celu zrestartowania konsoli HMC należy uruchomić komendę **chhmc -c altdiskboot -s enable --mode upgrade**.
 7. Zrestartuj konsolę HMC i uruchom aktualizację. W celu uruchomienia aktualizacji należy uruchomić komendę **hmcshutdown -r -t now**.

Zabezpieczanie konsoli HMC

Sekcja zawiera informacje na temat zwiększania bezpieczeństwa konsoli HMC przy zapewnieniu zgodności z korporacyjnymi standardami zabezpieczeń.

Poziom bezpieczeństwa konsoli HMC w konfiguracji domyślnej powinien być wystarczający dla większości użytkowników korporacyjnych. W przypadku konsoli HMC w wersji 8.4.0 lub późniejszej można dodatkowo zwiększyć bezpieczeństwo konsoli, stosując korporacyjne standardy zabezpieczeń. Aby zwiększyć bezpieczeństwo konsoli HMC, należy ustawić jej poziom bezpieczeństwa co najmniej na poziom 1. W zależności od środowiska i korporacyjnych wymagań dotyczących zabezpieczeń można też wybrać zabezpieczenia na poziomie 2 lub 3.

Uwaga: Przed zmianą poziomu zabezpieczeń należy porozumieć się z zespołem ds. zgodności zabezpieczeń korporacyjnych.

Zabezpieczenia poziomu 1

Aby zabezpieczyć konsolę HMC (ochrona poziomu 1), wykonaj następujące czynności:

1. Zmień predefiniowane hasło domyślnego użytkownika **hscroot**. Więcej informacji na temat strategii haseł sekcja [“Rozszerzona strategia haseł”](#) na stronie 94.
2. Jeśli konsola HMC nie należy do środowiska zabezpieczonego fizycznie, ustaw hasło grub, uruchamiając następującą komendę: **chhmc -c grubpasswd -s enable --passwd <nowe hasło grub>**
3. Jeśli na konsoli HMC został skonfigurowany zintegrowany moduł zarządzania (IMM), należy ustawić silne hasło modułu IMM.
4. Ustaw silne hasło dla użytkownika **admin** i zwykłych użytkowników na wszystkich serwerach.
5. Zaktualizuj konsolę HMC przy użyciu najnowszych poprawek bezpieczeństwa. Więcej informacji na temat poprawek bezpieczeństwa znajduje się w serwisie [IBM Fix Central](#).

Zabezpieczenia poziomu 2

Jeśli używanych jest wiele kont użytkowników, wykonaj następujące kroki, aby zwiększyć bezpieczeństwo konsoli HMC:

1. Utwórz na konsoli HMC osobne konto dla każdego użytkownika oraz przypisz użytkownikom wymagane role i zasoby. Więcej informacji na temat dostępnych ról użytkowników konsoli zawiera sekcja [Zadania, role użytkowników i identyfikatory na konsoli HMC](#) oraz związane z nimi komendy.

Uwaga: Upewnij się, że użytkownikom tworzonym na konsoli HMC przypisywane są wyłącznie niezbędne zasoby i role. W razie potrzeby można również tworzyć role niestandardowe.

2. Włącz replikację danych użytkowników między konsolami HMC. Replikacja danych użytkowników może być wykonywana w trybie podrzędnym lub równorzędnym. Więcej informacji na temat replikacji danych użytkowników znajduje się w sekcji [Zarządzanie replikacją danych](#).
3. Importuj certyfikat podpisany przez ośrodek certyfikacji.

Zabezpieczenia poziomu 3

Jeśli używanych jest wiele konsol HMC i kont administratorów systemu, wykonaj następujące kroki, aby zwiększyć bezpieczeństwo konsoli HMC:

1. Zastosuj scentralizowane uwierzytelnianie, na przykład z wykorzystaniem protokołu LDAP (Lightweight Directory Access Protocol) lub Kerberos. Więcej informacji na temat konfigurowania protokołu LDAP można znaleźć w sekcji [Konfigurowanie protokołu LDAP na konsoli HMC](#).
2. Włącz replikację danych użytkowników między konsolami HMC.
3. Upewnij się, że konsola HMC pracuje w [trybie NIST SP 800-131A](#), aby korzystała wyłącznie z silnych szyfrów.
4. Zablokuj nieużywane porty za pomocą firewalla. Informacje na temat portów konsoli HMC, których można używać, podano w poniższej tabeli:

Tabela 32. Port używany przez użytkownika do interakcji z konsolą HMC				
Port	Opis	Typ	Wersja protokołu (tryb domyślny)	Wersja protokołu (tryb NIST)
22	Open SSH	TCP	SSH v3	SSH v3
123	NTP	UDP	NTP	NTP
161	Agent SNMP	UDP	SNMP v3	SNMP v3
162	Pułapka SNMP	UDP	SNMP v3	SNMP v3
427	SLP	UDP	nie dotyczy	nie dotyczy
443	Interfejs GUI i interfejs API REST konsoli HMC	TCP	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)
657	RMC	TCP/UDP	RSCT (jawny tekst + skrót i podpis)	RSCT (jawny tekst + skrót i podpis)
2300	Terminal 5250 dla systemu IBM i	TCP	Jawny tekst	Jawny tekst
2301	Bezpieczny terminal 5250 dla systemu IBM i	TCP	TLS 1.2	TLS 1.2
5989	CIM (wcześniejszy port, nie działa)	TCP	Nie działa	Nie działa

Tabela 32. Port używany przez użytkownika do interakcji z konsolą HMC (kontynuacja)				
Port	Opis	Typ	Wersja protokołu (tryb domyślny)	Wersja protokołu (tryb NIST)
9900	FCS: wykrywanie między konsolami HMC	UDP	FCS	FCS
9920	FCS: komunikacja między konsolami HMC	TCP	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)
9960	Aplet VTerm w interfejsie GUI	TCP	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)
12443	Interfejs API REST konsoli HMC (wcześniejszy port)	TCP	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)
12347	Domena partnerska RSCT	UDP	RSCT (jawny tekst + skrót i podpis)	RSCT (jawny tekst + skrót i podpis)
12348	Domena partnerska RSCT	UDP	RSCT (jawny tekst + skrót i podpis)	RSCT (jawny tekst + skrót i podpis)

Uwagi:

- Kontakt z intranetem mogą mieć wyłącznie usługi SSH (port 22), HTTPS (port 443 i 12443), bezpieczny terminal 5250 dla IBM i (port 2301) oraz VTerm (port 9960). Wszystkie inne porty muszą być używane w sieci prywatnej lub odizolowanej. Można używać osobnego portu Ethernet i sieci VLAN dla usług RMC (Resource Monitoring and Control – port 657), FCS (port 9900 i 9920) oraz domeny partnerskiej RSCT (port 12347 i 12348).
- Porty wymienione w komendzie **netstat** są używane tylko do obsługi procesów wewnętrznych.

Rozszerzona strategia haseł

Za pomocą konsoli HMC można egzekwować wymagania dotyczące haseł dla użytkowników uwierzytelnianych lokalnie. Funkcja rozszerzonej strategii haseł pozwala administratorowi systemu na ustawianie ograniczeń dotyczących haseł. Rozszerzona strategia haseł ma zastosowanie w przypadku systemów z zainstalowaną konsolą HMC.

Administratorzy systemu mogą używać rozszerzonej strategii haseł do definiowania pojedynczej strategii haseł dla wszystkich użytkowników. Konsola HMC udostępnia strategię haseł o średnim poziomie zabezpieczeń, którą administratorzy systemu mogą aktywować w celu ustawienia ograniczeń dotyczących haseł. Administrator systemu może też wybrać aktywację strategii o średnim poziomie zabezpieczeń lub nowej strategii zdefiniowanej przez użytkownika. Strategii haseł o średnim poziomie zabezpieczeń konsoli HMC nie można usunąć z systemu. Poniższa tabela zawiera listę atrybutów strategii o średnim poziomie zabezpieczeń oraz wartości domyślne.

Tabela 33. Atrybuty hasła w przypadku strategii haseł o średnim poziomie zabezpieczeń konsoli HMC		
Atrybut	Opis	Wartość domyślna
min_pwage	Minimalna liczba dni, przez które hasło musi pozostać aktywne.	1

Tabela 33. Atrybuty hasła w przypadku strategii hasel o średnim poziomie zabezpieczeń konsoli HMC (kontynuacja)

Atrybut	Opis	Wartość domyślna
pwage	Maksymalna liczba dni, przez które hasło może pozostać aktywne.	180
min_length	Minimalna długość hasła.	8
hist_size	Liczba wcześniej zapisanych hasel, których nie można użyć ponownie.	10
warn_pwage	Liczba dni do wygaśnięcia hasła, gdy użytkownik otrzymuje ostrzeżenie o zbliżającym się wygaśnięciu.	7
min_digits	Minimalna liczba cyfr, jaka musi występować w hasle.	Brak
min_uppercase	Minimalna liczba wielkich liter.	1
min_lowercase	Minimalna liczba małych liter.	6
min_special_chars	Minimalna liczba znaków specjalnych, jaka musi występować w hasle.	Brak

Należy brać pod uwagę następujące kwestie dotyczące strategii hasel konsoli HMC o średnim poziomie zabezpieczeń:

- Strategia nie ma zastosowania do identyfikatorów użytkowników **hscroot**, **hscpe** i **root**.
- Strategia dotyczy tylko użytkowników uwierzytelnianych lokalnie i zarządzanych przez konsolę HMC. Nie można jej stosować do użytkowników LDAP ani Kerberos.
- Strategia hasel o średnim poziomie zabezpieczeń lub strategia zdefiniowana przez użytkownika konsoli HMC umożliwia administratorom systemu określanie ograniczeń dotyczącego ponownego wykorzystywania hasel.
- Hasło o średnim poziomie zabezpieczeń konsoli HMC to hasło tylko do odczytu. W przypadku hasła o średnim poziomie zabezpieczeń konsoli HMC nie można także zmieniać atrybutów. W celu ustawienia ograniczenia dotyczącego hasła można utworzyć nowe hasło zdefiniowane przez użytkownika.

Do konfigurowania strategii hasel o średnim poziomie zabezpieczeń konsoli HMC można używać następujących komend:

mkpwdpolicy

Importuje strategię hasel z pliku zawierającego wszystkie jej parametry lub tworzy nową strategię hasel.

lspwdpolicy

Pokazuje wszystkie dostępne profile strategii hasel i wyszukuje określone parametry. Można także wyświetlić aktualnie aktywną strategię hasel.

rmpwdpolicy

Usuwa istniejącą, nieaktywną strategię hasel.

Uwaga: Nie można usunąć aktywnej strategii o średnim poziomie zabezpieczeń ani domyślnej strategii hasel dostępnej tylko do odczytu.

chpwdpolicy

Zmienia parametry nieaktywnej strategii hasel.

Profile zabezpieczeń: RODO i PCI-DSS (Payment Card Industry Data Security Standard)

Sekcja zawiera informacje na temat ochrony prywatności danych użytkowników w konsoli HMC.

Konsola HMC (Hardware Management Console) jest urządzeniem zamkniętym, które nie przechowuje żadnych danych posiadaczy kart. W związku z tym do konsoli HMC ma zastosowanie tylko pewien podzbiór wymagań i procedur oceny bezpieczeństwa informatycznego przewidzianych w standardzie PCI-DSS. Na konsoli HMC można instalować tylko zaufany kod dystrybuowany przez IBM. W razie ujawnienia słabych punktów zabezpieczeń w ramach procesu IBM PSIRT publikowane są poprawki tymczasowe. Wymagania i zalecenia obejmują następujące elementy:

Pytania dotyczące RODO

Tabela 34. Pytania dotyczące RODO . Tabela zawiera informacje na temat pytań związanych z RODO.	
Pytania	Odpowiedzi
Jakiego rodzaju dane są przechowywane na konsoli HMC?	Konsola HMC przechowuje informacje konfiguracyjne dotyczące sprzętu Power, informacje dotyczące wirtualizacji PowerVM oraz informacje o metrykach wydajności.
Czy konsola HMC przetwarza dane osobowe?	Użytkownik może podać informacje kontaktowe związane z funkcją zgłoszenia automatycznego. Podanie informacji kontaktowych na potrzeby funkcji zgłoszenia automatycznego jest opcjonalne.
Które konta predefiniowane są używane do administrowania konsolą HMC?	Użytkownik administracyjny systemu używa nazwy użytkownika <i>hscroot</i> .
Czy którekolwiek z kont w konsoli HMC odnosi się do konkretnej osoby?	Nie.
Czy konieczne jest podawanie danych osobowych w konsoli HMC?	Nie. Użytkownik nie musi podawać danych osobowych. Istnieje jednak możliwość opcjonalnego podania takich informacji.
Czy plik dziennika konsoli HMC zawiera jakiegokolwiek dane osobowe?	Nie.
Czy możliwe jest całkowite i trwałe usunięcie danych osobowych?	Tak. Należy zdekongfigurować funkcję zgłoszeń automatycznych.

Pytania dotyczące standardu PCI-DSS

Tabela 35. Pytania dotyczące standardu PCI-DSS . Tabela zawiera informacje na temat pytań związanych ze standardem PCI-DSS.	
Pytania	Odpowiedzi
Jak zainstalować i utrzymywać konfigurację firewalla, aby zapewnić ochronę danych posiadacza karty?	Konsola HMC nie przechowuje żadnych danych posiadaczy kart ani nie ma do nich dostępu. Konsola HMC ma natomiast konfigurację firewalla, którą użytkownik może kontrolować w celu włączania określonych portów.
Czy mogę używać podanych przez dostawcę wartości domyślnych haseł systemowych i innych parametrów zabezpieczeń?	Przed zainstalowaniem systemu w sieci należy zmienić wszystkie predefiniowane hasła użytkownika <i>hscroot</i> .

Tabela 35. Pytania dotyczące standardu PCI-DSS . Tabela zawiera informacje na temat pytań związanych ze standardem PCI-DSS. (kontynuacja)

Pytania	Odpowiedzi
W jaki sposób konsola HMC chroni przechowywane dane posiadacza karty?	Konsola HMC nie przechowuje żadnych danych posiadaczy kart ani nie ma do nich dostępu.
W jaki sposób konsola HMC szyfruje dane posiadacza karty, gdy dane są przesyłane przez otwarte sieci publiczne?	Konsola HMC nie przechowuje żadnych danych posiadaczy kart ani nie ma do nich dostępu.
Jak wygląda używanie i regularne aktualizowanie programów antywirusowych?	Konsola HMC jest zamkniętym urządzeniem. Oznacza to, że szkodliwe oprogramowanie nie może zainfekować konsoli HMC.
Jak tworzyć i utrzymywać bezpieczne systemy i aplikacje?	Należy ręcznie instalować w systemie wymagane poprawki pobrane z serwisu WWW IBM Fix Central . Na konsoli HMC można instalować tylko zaufany kod dystrybuowany przez IBM.
Czy konsola HMC ogranicza dostęp do danych posiadaczy kart?	Konsola HMC nie przechowuje żadnych danych posiadaczy kart ani nie ma do nich dostępu.
Jak przypisać unikalny identyfikator każdej osobie, która ma dostęp do komputera?	To wymaganie można wdrożyć, upewniając się, że nie ma żadnych współużytkowanych identyfikatorów i stosowane są obowiązujące strategie hasel.
W jaki sposób ograniczyć fizyczny dostęp do danych posiadacza karty?	Konsola HMC nie przechowuje żadnych danych posiadaczy kart ani nie ma do nich dostępu.
W jaki sposób śledzić i monitorować dostęp do zasobów sieciowych i danych posiadaczy kart?	Konsola HMC nie przechowuje żadnych danych posiadaczy kart ani nie ma do nich dostępu.
W jaki sposób konsola HMC testuje bezpieczeństwo systemu i procesów?	Do skanowania zabezpieczeń we wszystkich udostępnionych wersjach konsoli HMC używane są narzędzia skanujące. Stosowane narzędzia skanujące to między innymi: <i>Qualys</i> , <i>Nessus</i> , <i>testssl</i> , <i>ssllscan</i> i <i>ASoC</i> .
W jaki sposób utrzymywać strategię bezpieczeństwa, która uwzględnia bezpieczeństwo informacji pracowników i wykonawców?	Administrator systemu wyłącza zdalne logowanie użytkowników, aktywuje możliwość logowania się użytkownika tylko wtedy, gdy jest to niezbędne, oraz dezaktywuje możliwość logowania się użytkownika, gdy dostęp nie jest już wymagany.

Rozwiązywanie najczęstszych problemów podczas zabezpieczania konsoli HMC

Sekcja zawiera informacje na temat rozwiązywania niektórych problemów, które mogą wystąpić podczas zabezpieczania konsoli HMC.

Jak zabezpieczyć połączenie między konsolą HMC a systemem?

Konsola HMC jest podłączona do systemu za pośrednictwem procesora serwisowego FSP (Flexible Service Processor). Do zarządzania procesorem FSP i hiperwizorem Power używany jest zastrzeżony protokół binarny NETC (Network Client Protocol). Poniższa tabela pokazuje listę portów używanych przez konsolę HMC:

Tabela 36. Porty procesora FSP używane do interakcji z konsolą HMC

Port procesora FSP	Opis	Wersja protokołu (tryb domyślny)	Wersja protokołu (tryb NIST)
443	Advanced System Management Interface	HTTPS (TLS 1.2)	HTTPS (TLS 1.2)
30000	NETC	NETC (TLS 1.2). W przypadku starszego oprogramowania wbudowanego następuje powrót do protokołu SSLv3.	NETC (TLS 1.2)
30001	VTerm	NETC (TLS 1.2). W przypadku starszego oprogramowania wbudowanego następuje powrót do protokołu SSLv3.	NETC (TLS 1.2)

Jak zablokować konsolę HMC?

Aby zwiększyć bezpieczeństwo infrastruktury, można użyć urządzenia IPS (Intrusion Prevention System) lub umieścić wszystkie konsole HMC i serwery IBM Power Systems za firewallem. Można też wyłączyć usługi sieciowe na konsoli HMC, jeśli konsola nie jest używana zdalnie lub planowane jest jej maksymalne zabezpieczenie. Aby wyłączyć usługi sieciowe na konsoli HMC, wykonaj następujące kroki:

1. Wyłącz zdalne wykonywanie komend, korzystając z portu SSH.
2. Wyłącz zdalny terminal wirtualny (port VTerm).
3. Wyłącz zdalny dostęp przez WWW (graficzny interfejs użytkownika konsoli HMC i interfejs API REST).
4. Zablokuj porty w firewallu, stosując odpowiednie ustawienia sieciowe konsoli HMC dla poszczególnych skonfigurowanych portów ethernetowych.

Jak ustawić na konsoli HMC tryb zgodności NIST SP 800-131A?

W przypadku konsoli HMC w wersji 8.1.0 lub nowszej przestawienie konsoli w tryb zgodności oznacza, że obsługiwane są tylko silne szyfry wymienione w publikacji NIST SP 800-131A. Może to uniemożliwić łączenie się ze starszymi serwerami Power Systems, na przykład serwerami POWER5 nieobsługującymi protokołu Transport Layer Security (TLS 1.2). Więcej informacji na temat zmiany trybu zabezpieczeń zawiera sekcja Tryb NIST konsoli HMC V8R8.

Jak można wyświetlać i zmieniać szyfry używane przez konsolę HMC?

Konsola HMC w wersji 8.1.0 lub nowszej obsługuje bezpieczniejsze zestawy algorytmów szyfrowania zdefiniowane w publikacji NIST 800-131A. W trybie domyślnym używane są tylko silne szyfry. Aby uzyskać więcej informacji na temat algorytmów szyfrowania używanych przez konsolę HMC, należy uruchomić komendę **lshmcencr**. Jeśli standardy korporacyjne wymagają użycia innego zestawu szyfrów, należy uruchomić komendę **chhmcencr** w celu zmodyfikowania algorytmów szyfrowania.

Aby wyświetlić algorytmy szyfrowania używane przez konsolę HMC do szyfrowania hasła użytkownika, uruchom następującą komendę:

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

Aby wyświetlić algorytmy szyfrowania, które mogą być obecnie używane przez interfejs WWW i interfejs API REST konsoli HMC, uruchom następującą komendę:


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

Aby wyświetlić algorytmy szyfrowania i algorytm MAC, które mogą być obecnie używane przez interfejs SSH konsoli HMC, uruchom następującą komendę:

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

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

Jak sprawdzić siłę certyfikatu na konsoli HMC?

Samopodpisane certyfikaty na konsoli HMC używają algorytmu SHA256 z silnym, 2048-bitowym szyfrowaniem RSA. Jeśli używane są certyfikaty podpisane przez ośrodek CA, należy upewnić się, że nie jest używane słabe szyfrowanie 1024-bitowe. Dla konsoli HMC można używać następujących certyfikatów:

- Certyfikatu podpisanego przez ośrodek CA można używać dla graficznego interfejsu użytkownika i interfejsu API REST konsoli HMC (porty 443 i 12443).
- Port 9920 jest używany do komunikacji między konsolami HMC. Tego certyfikatu nie można zastąpić własnym.

Jak wybrać opcję stosowania certyfikatu samopodpisanego (domyślnie) lub certyfikatu podpisanego przez ośrodek CA?

Konsola HMC automatycznie generuje certyfikat podczas instalacji. Można jednak wygenerować z konsoli HMC żądanie podpisania certyfikatu (CSR) i uzyskać nowy certyfikat wystawiony przez ośrodek certyfikacji. Taki certyfikat można importować do konsoli HMC. Należy pamiętać, aby uzyskać również nazwę domeny dla konsoli HMC. Więcej informacji na temat zarządzania certyfikatami w konsoli HMC zawiera sekcja [Zarządzanie certyfikatami](#).

Jak kontrolować działanie konsoli HMC?

Kontrola na konsolach HMC dotyczy przede wszystkim skonfigurowanych szyfrów oraz działań poszczególnych użytkowników konsoli HMC. Następujące komendy umożliwiają wyświetlanie informacji o działaniach poszczególnych użytkowników konsoli HMC:

Tabela 37. Szyfry używane przez konsolę HMC	
Przeznaczenie	Komenda
Szyfrowanie hasła (ustawienie globalne)	<code>lshmcencr -c passwd -t c</code>
Szyfrowanie hasła dla poszczególnych użytkowników	<code>lshmcusr -Fname:password_encryption</code>
Szyfry SSH	<code>lshmcencr -c ssh -t c</code>
Algorytmy MAC SSH	<code>lshmcencr -c sshmac -t c</code>
Szyfry używane na potrzeby graficznego interfejsu użytkownika i interfejsu API REST konsoli HMC	<code>lshmcencr -c webui -t c</code>

Następujące komendy umożliwiają monitorowanie różnych zdarzeń dotyczących konsoli HMC i zdarzeń serwisowalnych dla potrzeb pracy z konsolą:

Tabela 38. Komendy służące do wyświetlania zalogowanych użytkowników, zdarzeń konsoli i zdarzeń serwisowalnych na konsoli HMC	
Informacja	Komenda
Użytkownicy interfejsu GUI	<code>lslogon -r webui -u</code>

Tabela 38. Komendy służące do wyświetlania zalogowanych użytkowników, zdarzeń konsoli i zdarzeń serwisowalnych na konsoli HMC (kontynuacja)

Informacja	Komenda
Zadania interfejsu GUI	<code>lslogon -r webui -t</code>
Użytkownicy interfejsu CLI	<code>lslogon -r ssh -u</code>
Zadania interfejsu CLI	<code>lslogon -r ssh -t</code>
Operacje na konsoli HMC	<code>lssvcevents -t console -d <liczba dni></code>
Operacje na systemie	<code>lssvcevents -t hardware -m <system zarządzany> -d <liczba dni></code>

Zdarzenia monitorowania scentralizowanego dla konsoli HMC: jeśli używanych jest wiele konsol HMC, należy skonfigurować plik `rsyslog` w sposób umożliwiający gromadzenie wszystkich danych na temat użytkownika.

W jaki sposób IBM eliminuje słabe punkty zabezpieczeń konsoli HMC?

IBM stosuje proces reagowania na incydenty związane z bezpieczeństwem oparty na zespole IBM PSIRT (Product Security Incident Response Team). Globalny zespół IBM PSIRT odpowiada za przyjmowanie, sprawdzanie i wewnętrzne koordynowanie wszelkich informacji dotyczących słabych punktów zabezpieczeń produktów IBM. Wszystkie komponenty dostarczane z konsolą HMC, w tym zarówno komponenty Open Source, jak i opracowane przez IBM, są czynnie monitorowane i analizowane. IBM udostępnia poprawki tymczasowe i poprawki bezpieczeństwa dla wszystkich obsługiwanych wersji konsoli HMC.

Jak śledzić dostępność nowych poprawek tymczasowych na konsoli HMC?

Informacje o słabych punktach zabezpieczeń i poprawkach tymczasowych dla obsługiwanych wersji konsoli HMC są zamieszczane w biuletynach bezpieczeństwa. Aby śledzić poprawki tymczasowe na konsoli HMC, można:

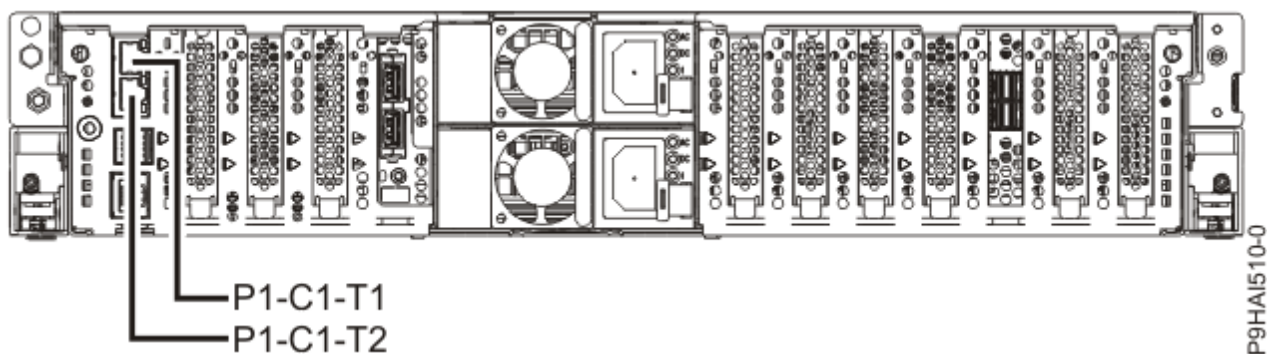
- Szukać najnowszych biuletynów bezpieczeństwa na stronie [biuletynów bezpieczeństwa IBM](#).
- Obserwować konto [@IBMPowereSupp](#) w serwisie Twitter, aby otrzymywać powiadomienia.
- Subskrybować powiadomienia e-mail na stronie [działu wsparcia IBM](#).

Położenie portów konsoli HMC

Położenie portów można ustalić za pomocą kodów położenia. Ilustracje położenia portów konsoli HMC umożliwiają odwzorowanie kodu położenia na pozycję portu konsoli HMC na serwerze.

Położenie portów konsoli HMC w modelu 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H oraz 9223-22S

Niniejszy diagram i tabela zawierają odwzorowanie portów konsoli HMC na serwer 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H oraz 9223-22S.



Rysunek 10. Położenie portów konsoli HMC w serwerach 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H oraz 9223-22S

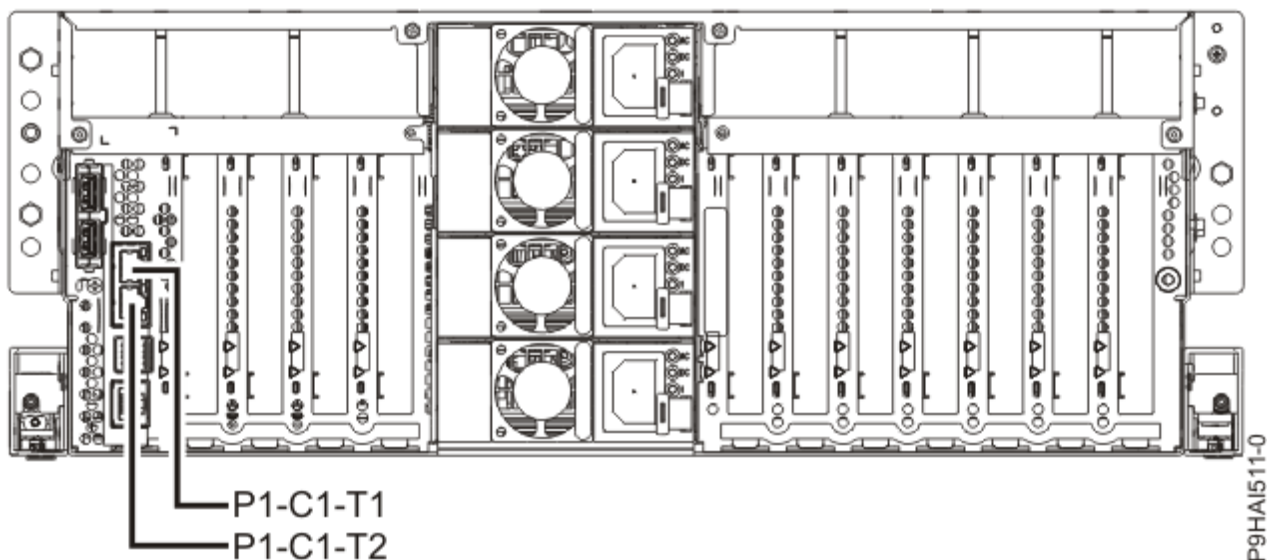
Tabela 39. Położenie portów konsoli HMC w serwerach 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H oraz 9223-22S

Port	Kod położenia fizycznego	Kontrolka identyfikacji
Port konsoli HMC 1	Un-P1-C1-T1	Nie
Port konsoli HMC 2	Un-P1-C1-T2	Nie

Więcej informacji o położeniach portów konsoli HMC w serwerze 5105-22E, 9008-22L, 9009-22A, 9009-22G, 9223-22H lub 9223-22S zawiera sekcja Położenie części i kody położenia w serwerach 9008-22L, 9009-22A, 9009-22G, 9223-22H lub 9223-22S.

Położenie portów konsoli HMC w modelu 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H oraz 9223-42S

Niniejszy diagram i tabela zawierają odwzorowanie portów konsoli HMC na serwer 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H oraz 9223-42S.



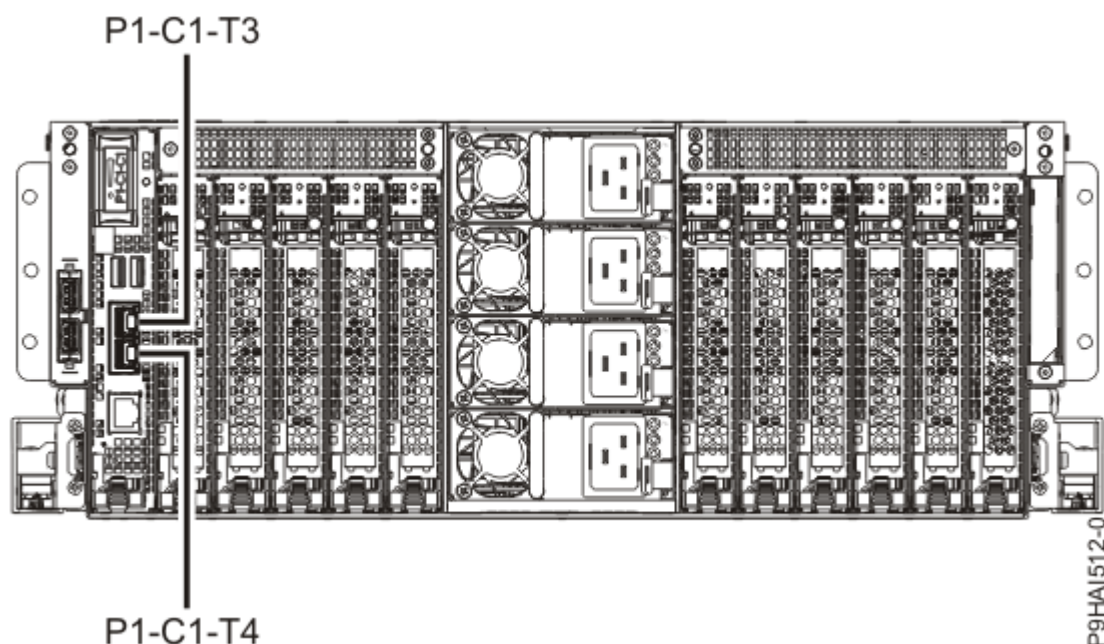
Rysunek 11. Położenie portów konsoli HMC w serwerach 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H oraz 9223-42S

Tabela 40. Położenie portów konsoli HMC w serwerach 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H oraz 9223-42S

Port	Kod położenia fizycznego	Kontrolka identyfikacji
Port konsoli HMC 1	Un-P1-C1-T1	Nie
Port konsoli HMC 2	Un-P1-C1-T2	Nie
Więcej informacji o położeniach portów konsoli HMC w serwerze 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H lub 9223-42S zawiera sekcja Położenie części i kody położenia w serwerach 9009-41A, 9009-41G, 9009-42A, 9009-42G, 9223-42H lub 9223-42S.		

Położenie portów konsoli HMC w modelu 9040-MR9

Poniższy diagram i tabela zawierają odwzorowanie portów konsoli HMC w serwerach 9040-MR9.



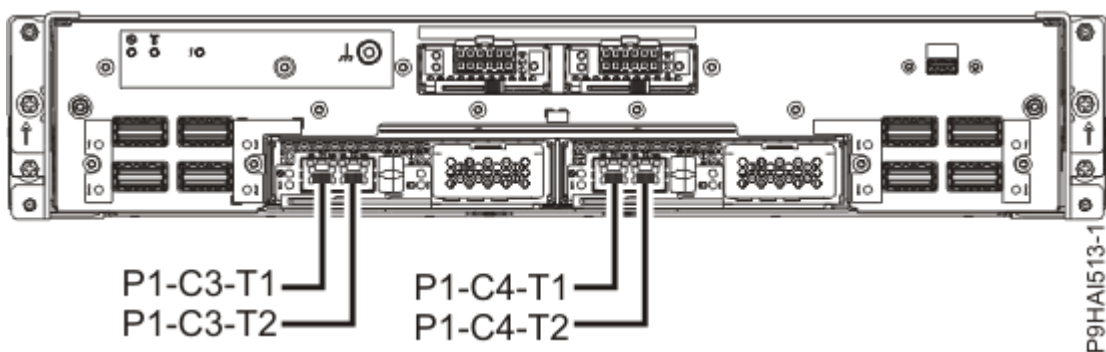
Rysunek 12. Położenie portów konsoli HMC w serwerach 9040-MR9

Tabela 41. Położenie portów konsoli HMC w serwerach 9040-MR9

Port	Kod położenia fizycznego	Kontrolka identyfikacji
Port konsoli HMC 1	Un-P1-C1-T3	Nie
Port konsoli HMC 2	Un-P1-C1-T4	Nie
Więcej informacji dotyczących położenia portów konsoli HMC w serwerach 9040-MR9 zawiera sekcja Położenie części i kody położenia.		

Położenie portów konsoli HMC w modelu 9080-M9S

Poniższy diagram i tabela zawierają odwzorowanie portów konsoli HMC w serwerach 9080-M9S.



Rysunek 13. Położenie portów konsoli HMC w serwerach 9080-M9S

Tabela 42. Położenie portów konsoli HMC w serwerach 9080-M9S

Port	Położenie portu fizycznego	Kontrolka identyfikacji
Karta procesora serwisowego 1 – port 1 konsoli HMC	Un-P1-C3-T1	Nie
Karta procesora serwisowego 1 – port 2 konsoli HMC	Un-P1-C3-T2	Nie
Karta procesora serwisowego 2 – port 1 konsoli HMC	Un-P1-C4-T1	Nie
Karta procesora serwisowego 2 – port 2 konsoli HMC	Un-P1-C4-T2	Nie
Więcej informacji dotyczących położenia portów konsoli HMC w serwerach 9080-M9S zawiera sekcja Położenie części i kody położenia .		

Uwagi

Niniejsza publikacja została przygotowana z myślą o produktach i usługach oferowanych w Stanach Zjednoczonych.

IBM może nie oferować w innych krajach produktów, usług lub opcji omawianych w tej publikacji. Informacje o produktach i usługach dostępnych w danym kraju/regionie można uzyskać od lokalnego przedstawiciela IBM. Odwołanie do produktu, programu lub usługi IBM nie oznacza, że można użyć wyłącznie tego produktu, programu lub usługi IBM. Zamiast nich można zastosować ich odpowiednik funkcjonalny pod warunkiem, że nie narusza to praw własności intelektualnej IBM. Jednakże cała odpowiedzialność za ocenę przydatności i sprawdzenie działania produktu, programu lub usługi, pochodzących od producenta innego niż IBM, spoczywa na użytkowniku.

IBM może posiadać patenty lub złożone wnioski patentowe na towary i usługi, o których mowa w niniejszej publikacji. Przedstawienie niniejszej publikacji nie daje żadnych uprawnień licencyjnych do tychże patentów. Zapytania dotyczące licencji można wysłać na piśmie na adres:

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

INTERNATIONAL BUSINESS MACHINES CORPORATION DOSTARCZA TĘ PUBLIKACJĘ W STANIE, W JAKIM SIĘ ZNAJDUJE ("AS IS"), BEZ UDZIELANIA JAKICHKOLWIEK GWARANCJI (W TYM TAKŻE RĘKOJMI), WYRAŻNYCH LUB DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ, PRZYDATNOŚCI DO OKREŚLONEGO CELU ORAZ GWARANCJI, ŻE PUBLIKACJA TA NIE NARUSZA PRAW OSÓB TRZECICH. Ustawodawstwa niektórych krajów nie dopuszczają zastrzeżeń dotyczących gwarancji wyraźnych lub domniemanych w odniesieniu do pewnych transakcji; w takiej sytuacji powyższe zdanie nie ma zastosowania.

Informacje zawarte w niniejszej publikacji mogą zawierać nieścisłości techniczne lub błędy drukarskie. Informacje te są okresowo aktualizowane, a zmiany te zostaną ujęte w kolejnych wydaniach tej publikacji. IBM zastrzega sobie prawo do wprowadzania ulepszeń i/lub zmian w produktach i/lub programach opisanych w tej publikacji w dowolnym czasie, bez wcześniejszego powiadomienia.

Wszelkie wzmianki w tej publikacji na temat stron internetowych innych podmiotów zostały wprowadzone wyłącznie dla wygody użytkownika i w żadnym wypadku nie stanowią zachęty do ich odwiedzania. Materiały dostępne na tych stronach nie są częścią materiałów opracowanych do tego produktu IBM, a użytkownik korzysta z nich na własną odpowiedzialność.

IBM ma prawo do używania i rozpowszechniania informacji przysłanych przez użytkownika w dowolny sposób, jaki uzna za właściwy, bez żadnych zobowiązań wobec ich autora.

Cytowane przykłady klientów oraz dane dotyczące wydajności mają charakter wyłącznie poglądowy. Rzeczywista wydajność w konkretnych konfiguracjach i środowiskach operacyjnych może być inna.

Informacje dotyczące produktów innych niż produkty IBM pochodzą od dostawców tych produktów, z opublikowanych przez nich zapowiedzi lub innych powszechnie dostępnych źródeł. Firma IBM nie testowała tych produktów i nie może potwierdzić dokładności pomiarów wydajności, kompatybilności ani żadnych innych danych związanych z tymi produktami. Pytania dotyczące produktów firm innych niż IBM należy kierować do dostawców tych produktów.

Stwierdzenia dotyczące przyszłych kierunków rozwoju i zamierzeń IBM mogą zostać zmienione lub wycofane bez powiadomienia.

Wszelkie ceny podawane przez IBM są sugerowanymi cenami detalicznymi; ceny te są aktualne i podlegają zmianom bez wcześniejszego powiadomienia. Ceny podawane przez dealerów mogą być inne.

Niniejsza informacja służy jedynie do celów planowania. Informacja ta podlega zmianom do chwili, gdy produkty, których ona dotyczy, staną się dostępne.

Publikacja ta zawiera przykładowe dane i raporty używane w codziennych operacjach działalności gospodarczej. W celu kompleksowego ich zilustrowania, podane przykłady zawierają nazwiska osób prywatnych, nazwy przedsiębiorstw oraz nazwy produktów. Wszystkie te nazwiska i nazwy są fikcyjne, a jakiegokolwiek ich podobieństwo do rzeczywistych osób i przedsiębiorstw jest całkowicie przypadkowe.

W przypadku przeglądania niniejszych informacji w formie elektronicznej, zdjęcia i kolorowe ilustracje mogą nie być wyświetlane.

Rysunki i specyfikacje zawarte w niniejszej publikacji nie mogą być kopiowane, tak w całości jak w części, bez pisemnej zgody IBM.

Informacje te zostały przygotowane przez IBM do wykorzystania na konkretnych wskazanych maszynach. IBM nie twierdzi, że informacje te mają służyć do innych celów.

Systemy komputerowe IBM zawierają mechanizmy zaprojektowane w celu zmniejszenia prawdopodobieństwa niewykrywalnego zniekształcenia lub utraty danych. Ryzyko takie nie może zostać jednakże całkowicie wyeliminowane. W przypadku nieplanowanego wyłączenia, awarii systemu, fluktuacji napięcia zasilającego, przerwy w zasilaniu lub uszkodzenia podzespołów należy zweryfikować dokładność operacji przeprowadzonych i danych zapisanych lub przekazanych przez system w czasie przerwy w zasilaniu lub awarii. Ponadto Użytkownicy zobowiązani są do opracowania procedur gwarantujących niezależną weryfikację danych przed wykorzystaniem ich w istotnych i newralgicznych operacjach. Zaleca się okresowe sprawdzanie na stronach WWW IBM bieżących informacji i poprawek właściwych dla systemu i dla odpowiadającego mu oprogramowania.

Oświadczenie o homologacji

Na terenie Twojego kraju produkt ten mógł nie być objęty certyfikacją w zakresie połączeń, za pomocą dowolnych środków, do interfejsów publicznych sieci telekomunikacyjnych. Proces certyfikacji dotyczący takich połączeń może być wymagany przepisami prawa w okresie późniejszym. W przypadku jakichkolwiek pytań należy kontaktować się z przedstawicielem lub resellerem IBM.

Ułatwienia dostępu dla serwerów IBM Power Systems

Ułatwienia dostępu pomagają użytkownikom niepełnosprawnym (na przykład mającym trudności z poruszaniem się lub niedowidzącym) w korzystaniu z produktów informatycznych.

Przegląd

Serwery IBM Power Systems zostały wyposażone w następujące istotne ułatwienia dostępu:

- Obsługa wyłącznie przy użyciu klawiatury
- Operacje przy użyciu lektora ekranowego

Serwery IBM Power Systems obsługują najnowszy standard W3C [WAI-ARIA 1.0](http://www.w3.org/TR/wai-aria/) (www.w3.org/TR/wai-aria/), aby zapewnić zgodność ze standardami zawartymi w dokumencie [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) i wytycznymi dotyczącymi treści WWW [Web Content Accessibility Guidelines \(WCAG\) 2.0](http://www.w3.org/TR/WCAG20/) (www.w3.org/TR/WCAG20/). Aby skorzystać z ułatwień dostępu, należy użyć najnowszej wersji lektora ekranowego i najnowszej wersji przeglądarki WWW, które są obsługiwane przez serwery IBM Power Systems.

Dokumentacja elektroniczna dotycząca serwerów IBM Power Systems dostępna w Centrum Wiedzy IBM zawiera również sekcję o ułatwieniach dostępu. W Centrum Wiedzy IBM ułatwienia dostępu zostały opisane w [sekcji dotyczącej ułatwień dostępu w pomocy Centrum Wiedzy IBM](http://www.ibm.com/support/knowledgecenter/doc/kc_help.html#accessibility) (www.ibm.com/support/knowledgecenter/doc/kc_help.html#accessibility).

Nawigacja za pomocą klawiatury

Ten produkt wykorzystuje standardowe klawisze nawigacyjne.

Informacje dotyczące interfejsu

Interfejsy użytkownika w serwerach IBM Power Systems nie zawierają treści migających z częstotliwością 2-55 razy na sekundę.

Interfejs WWW w serwerach IBM Power Systems korzysta z kaskadowego arkusza stylów, dzięki czemu treści są wyświetlane poprawnie i z odpowiednią jakością. Aplikacja umożliwia użytkownikom słabowidzącym korzystanie z systemowych ustawień ekranu, w tym z trybu wysokiego kontrastu. Można wybrać wielkość czcionki, zmieniając ustawienia urządzenia lub przeglądarki WWW.

Interfejs WWW w serwerach IBM Power Systems obsługuje nawigacyjne punkty orientacyjne WAI-ARIA, które umożliwiają szybką nawigację do obszarów funkcjonalnych w aplikacji.

Oprogramowanie innych dostawców

Serwery IBM Power Systems są wyposażone w niektóre programy innych dostawców, które nie podlegają umowie licencyjnej IBM. IBM nie składa żadnych oświadczeń dotyczących ułatwień dostępu w tych produktach. Aby uzyskać informacje na temat ułatwień dostępu w tych produktach, należy skontaktować się z ich dostawcami.

Informacje pokrewne dotyczące ułatwień dostępu

Oprócz zwykłych usług pomocy telefonicznej i serwisów wsparcia IBM, firma IBM udostępnia usługę pomocy telefonicznej z wykorzystaniem urządzeń TTY dla osób niesłyszących lub niedosłyszących, za pomocą której mają oni dostęp do usług sprzedaży i wsparcia:

Usługa pomocy telefonicznej TTY
800-IBM-3383 (800-426-3383)
(w Ameryce Północnej)

Więcej informacji o oferowanych przez IBM ułatwieniach dostępu można znaleźć w sekcji [Ułatwienia dostępu w produktach IBM](#) (www.ibm.com/able).

Postanowienia dotyczące ochrony prywatności

Oprogramowanie IBM, w tym rozwiązanie SaaS (Software as a Service), zwane dalej "Oferowanym Oprogramowaniem", może korzystać z informacji cookie lub z innych technologii w celu gromadzenia danych o używaniu produktów, poprawienia jakości usług dla użytkowników końcowych, dopasowania interakcji do ich oczekiwań oraz w innych celach. W wielu przypadkach Oferowane Oprogramowanie nie gromadzi informacji pozwalających na identyfikację osoby. Część Oferowanego Oprogramowania może jednak umożliwiać gromadzenie informacji pozwalających na identyfikację osoby. Jeśli Oferowane Oprogramowanie korzysta z informacji cookie do gromadzenia informacji pozwalających na identyfikację osoby, poniżej znajdują się szczegółowe informacje na temat takiego korzystania.

W zależności od wdrożonych konfiguracji Oferowane Oprogramowanie może korzystać z informacji cookie sesji, które gromadzą nazwę użytkownika i jego adres IP do celów zarządzania sesją. Informacje cookie można wyłączyć, ale może to spowodować odłączenie aktywowanych przez nie funkcjonalności.

Jeśli konfiguracje Oferowanego Oprogramowania umożliwiają gromadzenie informacji pozwalających na identyfikację użytkowników końcowych za pośrednictwem informacji cookie lub innych technologii, należy wystąpić o poradę prawną w zakresie prawa obowiązującego przy takim gromadzeniu danych, w tym wymagań dotyczących powiadomienia i zgody.

Więcej informacji na temat używania różnych technologii, w tym informacji cookie, do opisanych powyżej celów znajduje się w sekcji Ochrona prywatności w IBM pod adresem <http://www.ibm.com/privacy> oraz w Oświadczeniu IBM o Ochronie Prywatności pod adresem <http://www.ibm.com/privacy/details/us/en/> w sekcji zatytułowanej "Cookies, Web Beacons and Other Technologies".

Znaki towarowe

IBM, logo IBM oraz ibm.com są znakami towarowymi lub zastrzeżonymi znakami towarowymi International Business Machines Corporation zarejestrowanymi w wielu różnych krajach. Nazwy innych produktów i usług mogą być znakami towarowymi IBM lub innych podmiotów. Aktualna lista znaków towarowych IBM jest dostępna pod adresem [Copyright and trademark information](#) (Informacje o prawach autorskich i znakach towarowych).

Zastrzeżony znak towarowy Linux używany jest zgodnie z sublicencją Linux Foundation, wyłącznego licencjodawcy Linusa Torvaldsa, właściciela tego znaku na całym świecie.

Red Hat, JBoss, OpenShift, Fedora, Hibernate, Ansible, CloudForms, RHCA, RHCE, RHCSA, Ceph oraz Gluster są znakami towarowymi lub zastrzeżonymi znakami towarowymi Red Hat Inc. lub przedsiębiorstw podporządkowanych Red Hat Inc. w Stanach Zjednoczonych i innych krajach.

Microsoft i Windows są znakami towarowymi Microsoft Corporation w Stanach Zjednoczonych i/lub w innych krajach.

Znaki towarowe oraz loga Java i wszystkie oparte o Java są znakami towarowymi lub zastrzeżonymi znakami towarowymi Oracle i/lub przedsiębiorstw afiliowanych Oracle.

Uwagi dotyczące emisji promieniowania elektromagnetycznego

Uwagi dotyczące produktów klasy A

Poniższe oświadczenia dotyczące produktów klasy A mają zastosowanie do serwerów IBM z procesorami POWER9 oraz ich opcji, chyba że w informacjach dotyczących instalacji opcje zostały oznaczone jako produkty klasy B w zakresie kompatybilności elektromagnetycznej.

Podczas podłączania monitora do sprzętu należy użyć przeznaczonego do tego kabla oraz wszelkich urządzeń ograniczających zakłócenia, dostarczonych z monitorem.

Uwaga dla Kanady

CAN ICES-3 (A)/NMB-3(A)

Uwaga dla Wspólnoty Europejskiej i Maroka

Ten produkt jest zgodny z wymaganiami dotyczącymi bezpieczeństwa, zawartymi w dyrektywie 2014/30/UE w sprawie harmonizacji ustawodawstw państw członkowskich odnoszących się do kompatybilności elektromagnetycznej. IBM nie ponosi odpowiedzialności za błędy powstałe na skutek sprzecznego z zaleceniami, nieautoryzowanego wprowadzania zmian w produkcie, w tym dołączania kart opcjonalnych innych niż karty IBM.

This product may cause interference if used in residential areas. Such use must be avoided unless the user takes special measures to reduce electromagnetic emissions to prevent interference to the reception of radio and television broadcasts.

Warning: This equipment is compliant with Class A of CISPR 32. In a residential environment this equipment may cause radio interference.

Uwaga dla Niemiec

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, Deutschland
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.

Uwaga Japan Electronics and Information Technology Industries Association (JEITA)

(一社) 電子情報技術産業協会 高調波電流抑制対策実施
要領に基づく定格入力電力値: Knowledge Centerの各製品の
仕様ページ参照

This statement applies to products less than or equal to 20 A per phase.

高調波電流規格 JIS C 61000-3-2 適合品

This statement applies to products greater than 20 A, single phase.

高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。

- 回路分類 : 6 (単相、P F C回路付)
- 換算係数 : 0

This statement applies to products greater than 20 A per phase, three-phase.

高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。

- 回路分類 : 5 (3相、P F C回路付)
- 換算係数 : 0

Uwaga Japan Voluntary Control Council for Interference (VCCI)

この装置は、クラスA 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI-A

Uwaga dla Korei

이 기기는 업무용 환경에서 사용할 목적으로 적합성평가를 받은 기기로서 가정용 환경에서 사용하는 경우 전파간섭의 우려가 있습니다.

Uwaga dla Chińskiej Republiki Ludowej

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。

Uwaga dla Rosji

ВНИМАНИЕ! Настоящее изделие относится к классу A.
В жилых помещениях оно может создавать
радиопомехи, для снижения которых необходимы
дополнительные меры

Uwaga dla Tajwanu

警告使用者：
此為甲類資訊技術設備，
於居住環境中使用時，可
能會造成射頻擾動，在此
種情況下，使用者會被要
求採取某些適當的對策。

IBM Taiwan Contact Information:

台灣IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

Uwaga Federal Communications Commission (FCC) dla Stanów Zjednoczonych

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case the user will be required to correct the interference at his own expense.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. Proper cables and connectors are available from IBM-authorized dealers. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:

(1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Responsible Party:

International Business Machines Corporation

New Orchard Road

Armonk, NY 10504

Contact for FCC compliance information only: fccinfo@us.ibm.com

Uwagi dotyczące produktów klasy B

Poniższe oświadczenia dotyczące produktów klasy B mają zastosowanie do opcji oznaczonych w informacjach dotyczących instalacji opcji jako produkty klasy B w zakresie kompatybilności elektromagnetycznej (EMC).

Podczas podłączania monitora do sprzętu należy użyć przeznaczonego do tego kabla oraz wszelkich urządzeń ograniczających zakłócenia, dostarczonych z monitorem.

Uwaga dla Kanady

CAN ICES-3 (B)/NMB-3(B)

Uwaga dla Wspólnoty Europejskiej i Maroka

Ten produkt jest zgodny z wymaganiami dotyczącymi bezpieczeństwa, zawartymi w dyrektywie 2014/30/UE w sprawie harmonizacji ustawodawstw państw członkowskich odnoszących się do kompatybilności elektromagnetycznej. IBM nie ponosi odpowiedzialności za błędy powstałe na skutek sprzecznego z zaleceniami, nieautoryzowanego wprowadzania zmian w produkcie, w tym dołączania kart opcjonalnych innych niż karty IBM.

Uwaga dla Niemiec

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, Deutschland
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

Uwaga Japan Electronics and Information Technology Industries Association (JEITA)

(一社) 電子情報技術産業協会 高調波電流抑制対策実施 要領に基づく定格入力電力値: Knowledge Centerの各製品の 仕様ページ参照
--

This statement applies to products less than or equal to 20 A per phase.

高調波電流規格 JIS C 61000-3-2 適合品

This statement applies to products greater than 20 A, single phase.

高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。

- 回路分類 : 6 (単相、P F C回路付)
- 換算係数 : 0

This statement applies to products greater than 20 A per phase, three-phase.

高調波電流規格 JIS C 61000-3-2 準用品

本装置は、「高圧又は特別高圧で受電する需要家の高調波抑制対策ガイドライン」対象機器（高調波発生機器）です。

- 回路分類 : 5 (3相、P F C回路付)
- 換算係数 : 0

Uwaga Japan Voluntary Control Council for Interference (VCCI)

この装置は、クラスB情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをして下さい。

VCCI-B

Uwaga dla Tajwanu

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

Uwaga Federal Communications Commission (FCC) dla Stanów Zjednoczonych

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.

- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult an IBM-authorized dealer or service representative for help.

Properly shielded and grounded cables and connectors must be used in order to meet FCC emission limits. Proper cables and connectors are available from IBM-authorized dealers. IBM is not responsible for any radio or television interference caused by using other than recommended cables and connectors or by unauthorized changes or modifications to this equipment. Unauthorized changes or modifications could void the user's authority to operate the equipment.

This device complies with Part 15 of the FCC rules. Operation is subject to the following two conditions:

(1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Responsible Party:

International Business Machines Corporation
New Orchard Road
Armonk, New York 10504
Contact for FCC compliance information only: fccinfo@us.ibm.com

Warunki

Zezwolenie na korzystanie z tych publikacji jest przyznawane na poniższych warunkach.

Zakres stosowania: Niniejsze warunki stanowią uzupełnienie warunków używania serwisu WWW IBM.

Użytek osobisty: Użytkownik ma prawo kopiować te publikacje do własnego, niekomercyjnego użytku pod warunkiem zachowania wszelkich uwag dotyczących praw własności. Użytkownik nie ma prawa dystrybuować ani wyświetlać tych publikacji czy ich fragmentów, ani też wykonywać na ich podstawie prac pochodnych bez wyraźnej zgody IBM.

Użytek służbowy: Użytkownik ma prawo kopiować te publikacje, dystrybuować je i wyświetlać wyłącznie w ramach przedsiębiorstwa Użytkownika pod warunkiem zachowania wszelkich uwag dotyczących praw własności. Użytkownik nie ma prawa wykonywać na podstawie tych publikacji ani ich fragmentów prac pochodnych, kopiować ich, dystrybuować ani wyświetlać poza przedsiębiorstwem Użytkownika bez wyraźnej zgody IBM.

Prawa: Z wyjątkiem zezwoleń wyraźnie udzielonych w niniejszych publikacjach, nie udziela się jakichkolwiek innych zezwoleń, licencji ani praw, wyraźnych czy domniemanych, odnoszących się do tychże publikacji oraz informacji, danych, oprogramowania lub innej własności intelektualnej, w nich zawartych.

IBM zastrzega sobie prawo do anulowania zezwolenia przyznanego w publikacjach w każdej sytuacji, gdy uzna, że korzystanie z informacji w nich zawartych jest dla niego szkodliwe lub warunki w nich określone nie są przestrzegane.

Użytkownik ma prawo pobierać, eksportować lub reeksportować niniejsze informacje pod warunkiem zachowania bezwzględnej i pełnej zgodności z obowiązującym prawem i przepisami, w tym ze wszelkimi prawami i przepisami eksportowymi Stanów Zjednoczonych.

IBM NIE UDZIELA JAKICHKOLWIEK GWARANCJI, W TYM TAKŻE RĘKOJMI, DOTYCZĄCYCH TREŚCI TYCH PUBLIKACJI. PUBLIKACJE SĄ DOSTARCZANE W STANIE, W JAKIM SIĘ ZNAJDUJĄ ("AS IS") BEZ UDZIELANIA JAKICHKOLWIEK GWARANCJI, W TYM TAKŻE RĘKOJMI, WYRAŹNYCH CZY DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ, PRZYDATNOŚCI DO OKREŚLONEGO CELU ORAZ NIENARUSZANIA PRAW STRON TRZECICH.

