

Power Systems

ハードウェア管理コンソールの管理



お願い

本書および本書で紹介する製品をご使用になる前に、[121 ページの『特記事項』](#)に記載されている情報をお読みください。

本装置は、高調波電流規格 JIS C 61000-3-2 に適合しています。

本製品およびオプションに電源コード・セットが付属する場合は、それぞれ専用のものになっていますので他の電気機器には使用しないでください。本体機器提供後に、追加で電源コード・セットが必要となった場合は、補修用の取扱いとなります。

本書は、IBM ハードウェア管理コンソールのバージョン 9 リリース 2 保守レベル 950 および新版で明記されていない限り、以降のすべてのリリースおよびモディフィケーションに適用されます。

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原典：

Power Systems
Managing the Hardware Management
Console

発行：

日本アイ・ビー・エム株式会社

担当：

トランスレーション・サービス・センター

© Copyright International Business Machines Corporation 2017, 2020.

目次

HMC の管理	1
HMC の管理の新機能	1
HMC の概要	2
HMC で PowerSC MFA が構成されている場合のハードウェア管理コンソール (HMC) へのログ オン	3
定義済みユーザー ID およびパスワード	4
Web ベース・ユーザー・インターフェースの使用	4
メニュー・オプションの概要	5
タスクおよびロール	8
HMC タスク、ユーザー・ロール、ID、および関連コマンド	9
セッション処理	28
管理対象システムの「バージョン不一致」状態	29
システム管理 (サーバー)	30
システム・コンテンツ・ペイン	30
操作	31
アテンション LED	35
接続	36
システムのテンプレート	37
更新	38
レガシー	40
区画の作成	42
属性	43
PowerVM	45
Capacity on Demand	46
保守容易性	47
トポロジー・ダイアグラム	55
システム管理 (区画)	57
区画コンテンツ・ペイン	57
区画の属性	58
デフォルト・プロファイルの変更	59
操作	59
区画のテンプレート	64
プロファイル	64
区画の削除	65
保守容易性	65
仮想 I/O	67
システム管理 (フレーム)	69
属性	69
操作	70
構成	71
接続	71
保守容易性	72
グループの管理	74
Power エンタープライズ・プール	75
HMC 管理タスク	75
ガイド付きセットアップ・ウィザードの起動	75
ネットワーク・トポロジーの表示	76
ネットワーク接続性のテスト	76
ネットワーク設定の変更	77
パフォーマンス・モニター設定の変更	78
日付と時刻の変更	79

言語およびロケールの変更.....	79
ようこそテキストの作成.....	80
コンソールのデフォルト設定.....	80
シャットダウンまたは再始動.....	80
操作のスケジュール.....	81
ライセンスの表示.....	82
ハードウェア管理コンソールの更新.....	82
メディアのフォーマット設定.....	82
管理コンソール・データのバックアップ.....	83
管理コンソール・データの復元.....	84
アップグレード・データの保管.....	84
データ複製の管理.....	84
テンプレートおよび OS イメージ.....	85
すべてのシステム・プラン.....	88
ユーザーおよびセキュリティのタスク.....	89
ユーザー・パスワードの変更.....	89
ユーザー・プロファイルおよびアクセスの管理.....	90
ユーザーとタスクの管理.....	92
タスク・ロールおよびリソース・ロールの管理.....	93
証明書管理.....	94
証明書失効リストの管理.....	94
LDAP の管理.....	95
KDC の管理.....	96
MFA の管理.....	100
リモート・コマンド実行を有効にする.....	100
リモート操作を有効にする.....	101
リモート仮想端末を使用可能にする.....	101
保守容易性タスク.....	101
タスク・ログ.....	101
コンソール・イベント・ログ.....	102
サービス可能イベント・マネージャー.....	102
コール・ホーム機能用イベント・マネージャー (Events Manager for Call Home).....	102
サービス可能イベントの作成.....	103
ダンプの管理.....	103
サービス情報の送信.....	104
メディアのフォーマット設定.....	104
Electronic Service Agent セットアップ・ウィザード.....	105
ユーザーの許可.....	105
Electronic Service Agent の使用可能化.....	106
アウトバウンド接続の管理.....	106
インバウンド接続の管理.....	107
カスタマー情報の管理.....	107
イベント通知の管理.....	108
接続のモニタリング管理.....	108
リモート・オペレーション.....	109
リモート HMC の使用.....	109
Web ブラウザーの使用.....	110
HMC リモート・コマンド行の使用.....	112
LAN 接続 Web ブラウザーからの HMC のログイン.....	114
HMC を使用した OpenBMC ベースのシステムおよび BMC ベースのシステムの管理.....	114
管理対象システムの追加.....	114
システム管理 (サーバー).....	115
特記事項.....	121
IBM Power Systems サーバーのアクセシビリティ機能.....	122
プライバシー・ポリシーに関する考慮事項.....	123
プログラミング・インターフェース情報.....	124

商標.....	124
使用条件.....	124

HMC の管理

ハードウェア管理コンソール (HMC) の使用法について説明します。

このタスクについて

コンソールで使用できるタスクと、管理対象システムのグラフィカル・ビューおよび簡易ナビゲーション付きで Web ベースのユーザー・インターフェースを使用してナビゲートする方法について説明します。

注:ここにリストされている多くの HMC タスクは、PowerVC を使用して実行することもできます。PowerVC を使用して実行できるタスクについて詳しくは、[『HMC および PowerVC』](#)を参照してください。

HMC の管理の新機能

このトピック・コレクションの前の更新以降に、『HMC の管理』で新しく追加または大幅に変更された情報は次のとおりです。

2020 年 11 月

- 以下のトピックが追加されました。
 - [62 ページの『保守準備状況の検証』](#)
 - [87 ページの『Virtual I/O Server バックアップの管理』](#)
- 以下のトピックが更新されました。
 - [42 ページの『区画の作成』](#)
 - [48 ページの『サービス可能イベント・マネージャー』](#)
 - [51 ページの『FRU の追加』](#)
 - [52 ページの『FRU の交換』](#)
 - [52 ページの『FRU の除去』](#)
 - [57 ページの『区画コンテンツ・ペイン』](#)
 - [58 ページの『区画の属性』](#)
 - [65 ページの『サービス可能イベント・マネージャー』](#)

2020 年 5 月

- 以下のトピックが更新されました。
 - [9 ページの『HMC タスク、ユーザー・ロール、ID、および関連コマンド』](#)
 - [86 ページの『区画のテンプレート』](#)
 - [68 ページの『ハードウェア仮想化 I/O』](#)

2020 年 2 月

以下のトピックが更新されました。

- [86 ページの『VIOS イメージ』](#)

2019 年 11 月

- 以下のトピックが追加されました。
 - [3 ページの『HMC で PowerSC MFA が構成されている場合のハードウェア管理コンソール \(HMC\) へのログオン』](#)

- 以下のトピックが更新されました。
 - [2 ページの『HMC の概要』](#)
 - [4 ページの『定義済みユーザー ID およびパスワード』](#)
 - [58 ページの『区画の属性』](#)
 - [68 ページの『ハードウェア仮想化 I/O』](#)
 - [80 ページの『コンソールのデフォルト設定』](#)
 - [83 ページの『管理コンソール・データのバックアップ』](#)
 - [86 ページの『区画のテンプレート』](#)
 - [93 ページの『タスク・ロールおよびリソース・ロールの管理』](#)
 - [108 ページの『イベント通知の管理』](#)

2019 年 5 月

- 以下のトピックが追加されました。
 - [59 ページの『Netboot』](#)
 - [74 ページの『グループの管理』](#)
- 以下のトピックが更新されました。
 - [30 ページの『システム・コンテンツ・ペイン』](#)
 - [42 ページの『区画の作成』](#)
 - [44 ページの『プロセッサ、メモリー、I/O』](#)
 - [57 ページの『区画コンテンツ・ペイン』](#)
 - [89 ページの『ユーザー・パスワードの変更』](#)

2018 年 8 月

- 以下のトピックが追加されました。
 - [100 ページの『MFA の管理』](#)
 - [80 ページの『コンソールのデフォルト設定』](#)
 - [114 ページの『HMC を使用した OpenBMC ベースのシステムおよび BMC ベースのシステムの管理』](#)
- [77 ページの『ネットワーク設定の変更』](#) のトピックが更新されました。

2017 年 12 月

- POWER9™ プロセッサを搭載した IBM Power Systems サーバー上の HMC バージョン 9、リリース 1 以降に関する情報が追加されました。

HMC の概要

ハードウェア管理コンソール (HMC) の概念および機能のいくつか、およびそれらの機能にアクセスするために使用されるユーザー・インターフェースについて説明します。

HMC では、サーバーを構成および管理できます。1 つの HMC で複数のサーバーを管理でき、二重 HMC では同じシステムを管理することによって予備のサポートを提供できます。一貫性のある機能が実現されるように、各 HMC は、HMC ライセンス交付済みマシン・コード バージョン 9、リリース 1 がインストール済みの状態で出荷されます。

柔軟性と可用性を得るために、複数の構成の中で HMC をインプリメントできます。

DHCP サーバーとしての HMC

いずれかのプライベート・ネットワークを使用して HMC が管理するシステムに接続された HMC は、そのシステムのサービス・プロセッサ用 DHCP サーバーであることができます。HMC は、オープン・

ネットワーク上でシステムを管理しても構いません。この場合、管理対象システムのサービス・プロセッサ IP アドレスは、お客様提供の DHCP サーバーにより割り当て済みか、または Advanced System Management Interface (ASMI) を使用して手動割り当て済みです。

物理的な接近度

HMC バージョン 7 より前は、少なくとも 1 つのローカル HMC は管理対象システムに物理的に隣接して配置する必要があります。ローカル HMC の代替として、リモートで接続された HMC を介して操作するための接続と権限を備えた、パーソナル・コンピューターなどのサポート対象の装置を使用できます。ローカル装置は、サーバーと同じ部屋で、サーバーから 8 m (26 フィート) 離して設置する必要があります。ローカル装置には、HMC の代替となる同等の機能がなければなりません。この機能は、サービス担当員がシステムを保守するために必要です。仮想 HMC の場合、それらの機能には、ファームウェア更新や診断データなどのサービス・データおよびログ情報を HMC との間で転送する方式も含まれます。

冗長またはデュアル HMC

1 台または 2 台のハードウェア管理コンソールが 1 つのサーバーを管理しても構いません。2 台のハードウェア管理コンソールが 1 つのシステムを管理する場合、それらは対等であり、どちらの HMC を使用しても管理対象システムを制御することができます。ベスト・プラクティスとしては、1 台の HMC を管理対象システムのサポートされるネットワークまたは HMC ポートに接続することです。ネットワークが独立していることを意図しています。各 HMC は、サービス・ネットワークに対する DHCP サーバーであることができます。ネットワークが独立しているために、DHCP サーバーは 2 つのユニークかつルーティング不能な IP 範囲で IP アドレスを提供するようにセットアップされる必要があります。

同じサーバーを管理する冗長 HMC またはデュアル HMC は、バージョンおよびリリース・レベルが異なっていてはいけません。例えば、バージョン 7 リリース 7.1.0 の HMC とバージョン 7 リリース 3.5.0 の HMC では同じサーバーを管理できません。HMC 同士は同じバージョンとリリース・レベルでなければなりません。

サーバーが高位バージョンの管理コンソールに接続されると、区画の構成は最新のバージョンにアップグレードされます。区画の構成がアップグレードされた後は、下位レベルの管理コンソールではデータを正しく解釈できません。サーバーが高位バージョンの管理コンソールで管理された後で、下位バージョンの管理コンソールに戻るには、まずサーバーを初期化する必要があります。旧レベルで取り込まれたバックアップをリストアするか、区画を再作成することができます。サーバーが初期化されない場合、下位レベルの HMC のバージョンによっては、以下のいずれかの結果が発生することがあります。

- HMC バージョン 7 リリース 7.8.0 以降では、参照コード「**保管域バージョン不一致**」が付いた「**バージョン不一致**」の接続エラーが報告されます。
- HMC バージョン 7 リリース 7.7.0 以前では、「**不完全**」または「**リカバリー**」のサーバー状態が報告される場合があります。さらに、区画構成の破損が発生することもあります。

HMC で PowerSC MFA が構成されている場合のハードウェア管理コンソール (HMC) へのログイン

HMC で IBM PowerSC 多要素認証 (MFA) が構成されている場合に HMC にログインする方法について説明します。

HMC で IBM PowerSCMFA が有効になっていて、PowerSC MFA サーバーでユーザーが構成されている場合、最初にユーザー ID とセキュリティ管理者によって提供されているポリシー名を入力することで、HMC にログインすることができます。その後、追加の資格情報を求めるプロンプトが表示されます。

HMC のログイン・ページで「**ポリシー名**」をクリックすると、認証メカニズムはインバンド認証タイプに設定されます。例えば、使用するポリシーが Rivest-Shamir-Adleman (RSA) 認証方式に関連付けられている場合、RSA セキュア ID デバイスまたはアプリケーションから受け取ったセキュア ID パスコードを入力できます。次に、「**次へまたはサインイン**」をクリックして、HMC にログインします。

注:

- HMC で MFA が有効になっていない場合は、ユーザー ID とパスワードを使用して HMC にログインできます。
- セキュリティ管理者によって構成されている PowerSC MFA サーバーからキャッシュ・トークン資格情報 (CTC) コードを取得している場合は、「**パスワード**」フィールドに CTC コードを入力します。

定義済みユーザー ID およびパスワード

定義済みユーザー ID およびパスワードが、ハードウェア管理コンソール (HMC) に用意されています。システム・セキュリティ上、必ずユーザーはすぐに hscroot 事前定義パスワードを変更してください。

HMC にログインしようとするときにパスワードの有効期限が切れている場合は、以下のステップを実行します。

1. 「現在のパスワード」および「新規パスワード」を入力します。
2. 「新規パスワードの確認」フィールドに新規パスワードを再入力します。
3. 「了解」をクリックします。新規パスワードが現在のパスワード・ポリシーに準拠している場合、HMC のパスワードが変更されます。

次のような定義済みユーザー ID およびパスワードが、HMC に用意されています。

表 1. 定義済み HMC ユーザー ID およびパスワード		
ユーザー ID	パスワード	目的
hscroot	abc123	hscroot ユーザー ID およびパスワードは、初めて HMC にログインする際に使用します。これらは大/小文字の区別があり、スーパー管理者の ロールを持つメンバーのみが使用できます。

Web ベース・ユーザー・インターフェースの使用

Web ベースのユーザー・インターフェースを使用すると、ハードウェア管理コンソール (HMC) または管理対象リソース上でタスクを実行できます。

このユーザー・インターフェースは、タイトル・バー、ナビゲーション領域、コンテンツ・ペイン、メニュー・ポッド、およびドック・ポッドなど、いくつかの主要なコンポーネントから構成されています。

タイトル・バー は、ワークスペース・ウィンドウの上部を横切るもので、製品、ログインしているいずれかのユーザー、ヘルプ・オプション、およびロゴを示します。

ウィンドウの左側の部分にあるナビゲーション領域 には、システムを選択して HMC のタスクを開始するための 1 次ナビゲーション・リンクが含まれています。

ウィンドウの中央部分にあるコンテンツ・ペイン には、ナビゲーション領域での現在の選択に基づいた情報が表示されます。例えば、ナビゲーション領域で「**すべてのシステム**」が選択されている場合、使用可能なすべてのシステムがコンテンツ・ペインに表示されます。

ウィンドウの左側の部分にあるメニュー・ポッド は、システムを選択した後に表示され、よく使用される HMC タスクへの素早いアクセスとリソースおよび属性のビューを提供します。

ドック・ポッド はウィンドウの右側の部分にあり、ユーザーが選択した HMC タスクをピン留めするために使用できる「ピン留め」機能を表示します。この機能を使用して、それらのタスクに素早くアクセスすることができます。

HMC ワークスペースのペインのサイズは、作業ペインとナビゲーション・ペインの境界上でマウス・ポインターを、マウス・ポインターが 2 重ポイントの矢印に変わるまで動かすことによって、変更できます。ポインターの形が変わったら、マウスの左ボタンを押したまま、マウス・ポインターを左または右にドラッグします。ボタンを放すと、ナビゲーション・ペインまたは作業ペインのサイズが大きくなるか小さくなります。このタスクは、タスクパッドとリソース・テーブルを分ける作業ペインの境界内でも実行できます。

「ギャラリー・ビューの表示」、「テーブル・ビューの表示」、または「関係ビューの表示 (Display Relationship View)」をクリックすることで、設定に従ってコンテンツ・ペイン のレイアウトを変更することができます。

テーブルの列を選択して新しい位置にドラッグすることにより、列の位置を変更できます。また、各テーブルの最後の列の横にあるドロップダウン・メニューをクリックすることで、表示する列を選択すること

もできます。「**ユーザー設定の保存 (Save User Preferences)**」アイコンをクリックして、設定を保存することができます。

各表の下にある「**ページごとの項目数 (Items per page)**」(**10、20、30、または 50**) アイコンのいずれかををクリックすることで、各ページの表に表示される行数を変更することができます。

注: ポップアップ・ウィンドウは、HMC の全機能について使用可能になっている必要があります。

メニュー・オプションの概要

ハードウェア管理コンソール (HMC) で使用可能なメニュー・オプションと、それに関連するタスクについて説明します。

このセクションで説明するメニュー・オプションとタスクは、HMC インターフェースで使用可能です。

表 2. HMC のメニュー・オプション		
メニュー	サブメニュー	オプション/タスク
リソース 	すべてのシステム	すべてのシステムの表示
	すべてのパーティション	すべてのパーティションの表示
	すべての Virtual I/O Server	すべての Virtual I/O Server の表示
	すべてのフレーム	すべてのフレームの表示
	すべての Power エンタープライズ・プール	すべての Power エンタープライズ・プールの表示
	すべての共用ストレージ・プール・クラスター	すべての共用ストレージ・プール・クラスターの表示
	すべてのグループ	すべてのグループの表示

表 2. HMC のメニュー・オプション (続き)

メニュー	サブメニュー	オプション/タスク
HMC 管理 	コンソール設定	ガイド付きセットアップ・ウィザードの起動
		ネットワーク・トポロジーの表示
		ネットワーク接続性のテスト
		ネットワーク設定の変更
		パフォーマンス管理設定の変更
		日付と時刻の変更
		言語およびロケールの変更
	コンソール管理	管理コンソールのシャットダウンまたは再始動
		操作のスケジュール
		ライセンスの表示
		ハードウェア管理コンソールの更新
		インストール・リソースの管理
		Virtual I/O Server イメージ・リポジトリの管理
		メディアのフォーマット設定
		管理コンソール・データのバックアップ
		管理コンソール・データの復元
		アップグレード・データの保管
		データ複製の管理
	テンプレート・ライブラリー	システムおよびパーティション・ライブラリー
	更新	使用不可 (代わりに「ハードウェア管理コンソールの更新」オプションを使用する)

表 2. HMC のメニュー・オプション (続き)

メニュー	サブメニュー	オプション/タスク
ユーザーおよびセキュリティ 	ユーザーおよびロール	ユーザー・パスワードの変更
		ユーザー・プロファイルおよびアクセスの管理
		ユーザーとタスクの管理
		タスク・ロールおよびリソース・ロールの管理
	システムおよびコンソール・セキュリティ	証明書管理
		LDAP の管理
		KDC の管理
		リモート・コマンド実行を有効にする
		リモート操作を有効にする
		リモート仮想端末を使用可能にする

表 2. HMC のメニュー・オプション (続き)

メニュー	サブメニュー	オプション/タスク
保守容易性 	コンソール・イベント・ログ	「コンソール・イベントの表示」ウィンドウ
	サービス可能イベント・マネージャー	「サービス可能イベント・マネージャー」ウィンドウ
	コール・ホーム機能用イベント・マネージャー (Events Manager for Call Home)	「コール・ホーム用イベント・マネージャー」ウィンドウ
	サービス管理	サービス可能イベントの作成
		リモート接続の管理
		リモート・サポート要求の管理
		ダンプの管理
		サービス情報の送信
		サービス情報のスケジュール
		メディアのフォーマット 設定
		管理コンソール・トレースの実行
		管理コンソール・ログの表示
		コンポーネント・ログの表示
		Electronic Service Agent セットアップ・ウィザード
		ユーザーの許可
		Electronic Service Agent の使用可能化
		アウトバウンド接続の管理
		インバウンド接続の管理
		カスタマー情報の管理
		サービス可能イベント通知の管理
		接続のモニタリング管理

タスクおよびロール

各 HMC ユーザーは、異なるロールのメンバーになることができます。これらのロールはそれぞれ、ユーザーが HMC の異なる部分にアクセスして、管理対象システムで異なるタスクを完了できるようにします。HMC ロールは、事前定義またはカスタマイズされています。

説明するロールは HMC ユーザーに適用されます。論理区画上で稼働するオペレーティング・システムは、独自のセットのユーザーとロールを持ちます。HMC ユーザーを作成するとき、そのユーザーにタスク・ロールを割り当てなければなりません。各タスク・ロールによって、ユーザーは HMC インターフェース上で使用可能なタスクへのさまざまなレベルのアクセスができるようになります。HMC の各ユーザー役割が実行できるタスクに関して詳しくは、[9 ページの『HMC タスク、ユーザー・ロール、ID、および関連コマンド』](#)を参照してください。

個々の HMC ユーザーに管理対象システムおよび論理区画を割り当てることができます。このアクションによって、管理対象システム A にはアクセスできるが、管理対象システム B にはアクセスできないユーザー

ーを作成することができます。管理対象リソース・アクセスの各グループは、管理対象リソース・ロールと呼ばれます。

HMC のデフォルトである**定義済み HMC ロール**には、以下のようなものがあります。

表 3. 定義済み HMC ロール		
ロール	説明	HMC ユーザー ID
オペレーター	オペレーターは、日常のシステム操作を担当します。	hmcooperator
スーパー 管理者	スーパー 管理者が HMC システムの root ユーザーまたは管理者の役目を果たします。スーパー 管理者は、HMC システムの大部分にアクセスしてこれを変更する、無制限の権限を持っています。	hmcsuperadmin
プロダクト・エンジニア	プロダクト・エンジニアは、サポート状態を支援しますが、HMC ユーザー管理機能にアクセスすることはできません。システムへのサポート・アクセスを与えたい場合は、製品エンジニア・ロールを持つユーザー ID を作成して管理する必要があります。	
サービス担当者	サービス技術員とは、お客様の設置場所でシステムの設置、構成、または修理を担当する従業員です。	hmcservicerep
ビューアー	ビューアーは HMC 情報を表示できますが、構成情報を変更することはできません。	hmcviewer
クライアント・ライブ・アップデート	クライアント・ライブ・アップデートのロールは、管理対象システムの 1 つの区画に対して AIX Live Update 機能を使用することを目的としています。クライアント・ライブ・アップデートのユーザーは、AIX 上でライブ・アップデートを完了するのに必要なものに限った権限を持ちます。	hmcclientliveupdate

定義済み HMC ロールを変更して、**カスタマイズ HMC ロール**を作成することができます。カスタマイズ HMC ロールの作成は、特定のタスク特権を限られたユーザーに付与したり制限したりするのに有用です。

HMC タスク、ユーザー・ロール、ID、および関連コマンド

このセクションで説明するロールは HMC ユーザーに適用されます。論理区画上で稼働する オペレーティング・システムには、独自のセットのユーザーとロールがあります。

各 HMC ユーザーには関連するタスク・ロールとリソース・ロールがあります。タスク・ロールは、そのユーザーが実行可能な操作を定義します。リソース・ロールは、タスクを実行するためのシステムと区画を定義します。各ユーザーはタスク・ロールまたはリソース・ロールを共有しても構いません。HMC は 5 つの定義済みタスク・ロールを持ってインストールされます。単一の定義済みリソース・ロールにより、すべてのリソースにアクセスできるようになります。オペレーターは、カスタマイズされたタスク・ロール、カスタマイズされたリソース・ロール、およびカスタマイズされたユーザー ID を追加することができます。

一部のタスクには、関連コマンドがあります。HMC コマンド行へのアクセスについて詳しくは、[112 ページの『HMC リモート・コマンド行の使用』](#)を参照してください。

タスクによっては、コマンド行を使用しないと実行できないものがあります。該当するタスクのリストについては、[26 ページの表 9](#)を参照してください。

タスク情報の記載先については、以下の表を参照してください。

表 4. HMC タスクのグループ化	
HMC タスクおよび対応するユーザー・ロール、ID、およびコマンド	関連する表
HMC 管理	10 ページの表 5
サービス管理	13 ページの表 6
システム 管理	15 ページの表 7
コントロール・パネル機能	25 ページの表 8

以下の表は、HMC 管理タスク、コマンド、および各 HMC 管理タスクと関連するデフォルト・ユーザー・ロールを示します。

表 5. HMC 管理タスク、コマンド、およびデフォルト・ユーザー・ロール				
HMC インターフェース・タスクおよび関連コマンド	ユーザー・ロールおよび ID			
	オペレーター (hmcoperator)	スーパー 管理者 (hmcsuperadmin)	ビューアー (hmcviewer)	サービス担当員 (hmcservicerep)
83 ページの『管理コンソール・データのバックアップ』 bkconsdata	X	X		X
プロファイル・データのバックアップ bkprofdata	X	X		X
BMC 証明書の変更 chbmccert	X	X		X
証明書管理 chhmccert lshhmccert mkhmccert		X		
79 ページの『日付と時刻の変更』 chhmc lshmc	X	X		X
79 ページの『言語およびロケールの変更』 chhmc lshmc	X	X	X	X

表 5. HMC 管理タスク、コマンド、およびデフォルト・ユーザー・ロール (続き)

HMC インターフェース・タスクおよび関連コマンド	ユーザー・ロールおよび ID			
	オペレーター (hmcoperator)	スーパー 管理者 (hmcsuperadmin)	ビューアー (hmcviewer)	サービス担当員 (hmcservicerep)
HMC 構成の変更 chipsec chpsm chusrtca	X	X		X
77 ページの『ネットワーク設定の変更』 chhmc lshmc	X	X		X
プロキシー構成の変更 chproxy		X		X
89 ページの『ユーザー・パスワードの変更』 chhmcusr	X	X	X	X
BMC 証明書のリスト lsbmccert	X	X	X	X
HMC 構成のリスト lsipsec lpspm lsusrtca	X	X	X	X
HMC 暗号化タスクのリスト lshmcencr	X	X	X	
システム・プランのリスト lssysplan		X		
プロキシー構成のリスト lsproxy	X	X	X	X
96 ページの『KDC の管理』 chhmc lshmc getfile rmfile		X		

表 5. HMC 管理タスク、コマンド、およびデフォルト・ユーザー・ロール (続き)

HMC インターフェース・タスクおよび関連コマンド	ユーザー・ロールおよび ID			
	オペレーター (hmcoperator)	スーパー管理者 (hmcsuperadmin)	ビューアー (hmcviewer)	サービス担当員 (hmcservicerep)
95 ページの『LDAP の管理』 lshmcldap chhmcldap		X		
75 ページの『ガイド付きセットアップ・ウィザードの起動』		X		
リモート・ハードウェア管理コンソールの起動	X	X	X	X
HMC スクリーンのロック	X	X	X	X
ログオフまたは切断	X	X	X	X
94 ページの『証明書管理』		X		
84 ページの『データ複製の管理』	X	X		
93 ページの『タスク・ロールおよびリソース・ロールの管理』 chaccfg lsaccfg mkaccfg rmaccfg		X		
90 ページの『ユーザー・プロファイルおよびアクセスの管理』 chhmcusr lshmcusr mkhmcusr rmhmcusr		X		
92 ページの『ユーザーとタスクの管理』 lslogon termtask	X	X	X	X
5250 コンソールのオープン	X	X		X

表 5. HMC 管理タスク、コマンド、およびデフォルト・ユーザー・ロール (続き)

HMC インターフェース・タスク および関連コマンド	ユーザー・ロールおよび ID			
	オペレーター (hmcoperator)	スーパー管理者 (hmcsuperadmin)	ビューアー (hmcviewer)	サービス担当員 (hmcservicerep)
100 ページの『リモート・コマンド実行を有効にする』 chhmc lshmc	X	X		X
101 ページの『リモート操作を有効にする』 chhmc lshmc	X	X	X	X
101 ページの『リモート仮想端末を使用可能にする』	X	X		X
84 ページの『管理コンソール・データの復元』	X	X		X
84 ページの『アップグレード・データの保管』 saveupgdata	X	X		X
81 ページの『操作のスケジュール』	X	X		
80 ページの『シャットダウンまたは再始動』 hmcshutdown	X	X		X
48 ページの『サービス可能イベント・マネージャー』 lssvcevents	X	X		X
82 ページの『ライセンスの表示』	X	X	X	X

以下の表は、サービス管理タスク、コマンド、およびデフォルト・ユーザー・ロールを示します。

表 6. サービス管理タスク、コマンド、およびデフォルト・ユーザー・ロール

HMC インターフェース・タスク および関連コマンド	ユーザー・ロールおよび ID			
	オペレーター (hmcoperator)	スーパー管理者 (hmcsuperadmin)	ビューアー (hmcviewer)	サービス担当員 (hmcservicerep)
49 ページの『サービス可能イベントの作成』		X		X

表 6. サービス管理タスク、コマンド、およびデフォルト・ユーザー・ロール (続き)

HMC インターフェース・タスク および関連コマンド	ユーザー・ロールおよび ID			
	オペレーター (hmcoperator)	スーパー管理者 (hmcsuperadmin)	ビューアー (hmcviewer)	サービス担当員 (hmcservicerep)
102 ページの『サービス可能イベント・マネージャー』 chsvcevent cpfile lssvcevents mksvcevent updpmh		X		X
82 ページの『メディアのフォーマット設定』 formatmedia	X	X		X
103 ページの『ダンプの管理』 dump cpdump getdump lsdump startdump lsfru	X	X		X
104 ページの『サービス情報の送信』 chsacfg lssacfg	X	X		
106 ページの『Electronic Service Agent の使用可能化』	X	X		X
106 ページの『アウトバウンド接続の管理』	X	X		X
107 ページの『インバウンド接続の管理』	X	X		X
107 ページの『カスタマー情報の管理』	X	X		X
105 ページの『ユーザーの許可』		X		

表 6. サービス管理タスク、コマンド、およびデフォルト・ユーザー・ロール (続き)

HMC インターフェース・タスク および関連コマンド	ユーザー・ロールおよび ID			
	オペレーター (hmcoperator)	スーパー管理者 (hmcsuperadmin)	ビューアー (hmcviewer)	サービス担当員 (hmcservicerep)
108 ページの『イベント通知の 管理』 chsacfg lssacfg	X	X		X
108 ページの『接続のモニタリ ング管理』	X	X	X	X
105 ページの『Electronic Service Agent セットアップ・ウ ィザード』		X		X

以下の表は、システム管理タスク、コマンド、およびデフォルト・ユーザー・ロールを示します。

表 7. システム管理タスク、コマンド、およびデフォルト・ユーザー・ロール

HMC インターフェース・タスクおよび 関連コマンド	ユーザー・ロール/ID			
	オペレーター (hmcoperator)	スーパー管理者 (hmcsuperadmin)	ビューアー (hmcviewer)	サービス担当員 (hmcservicerep)
43 ページの『一般設定』 lshwres	X	X	X	X
lsled	X	X	X	X
lslparmigr	X	X	X	X
lssyscfg	X	X	X	X
chhwres	X	X	X	X
chsyscfg	X	X	X	X
migrpar	X	X	X	X
optmem	X	X		X
lsmemopt	X	X	X	X
lsrrstartlpar	X	X		
パスワードの更新 chsyspwd		X		
デフォルト・ユーザー・インターフェ ース設定の変更	X	X	X	X

表 7. システム管理タスク、コマンド、およびデフォルト・ユーザー・ロール (続き)

HMC インターフェース・タスクおよび 関連コマンド	ユーザー・ロール/ID			
	オペレーター (hmcoperator)	スーパー管理者 (hmcsuperadmin)	ビューアー (hmcviewer)	サービス担当員 (hmcservicerep)
CEC プロパティのリスト lscomgmt lsiotopo	X	X	X	X
使用状況データのリスト lslparutil	X	X	X	X
操作				
31 ページの『電源オフ』 chsysstate	X	X		X
59 ページの『活動化』 chsysstate	X	X		X
65 ページの『現在の構成の保管』 chsysstate	X	X		X
60 ページの『再始動』 chsysstate	X	X		X
60 ページの『シャットダウン』 chsysstate	X	X		X
chlparstate	X	X		X
LED 状況: アテンション LED の非活動化 35 ページの『アテンション LED』 chled	X	X		
LED 状況: LED の識別 35 ページの『アテンション LED』	X	X	X	X
LED 状況: LED のテスト 35 ページの『アテンション LED』	X	X	X	X
33 ページの『操作のスケジュール』	X	X		
35 ページの『ASM インターフェース の起動』 asmmenu	X	X		X

表 7. システム管理タスク、コマンド、およびデフォルト・ユーザー・ロール (続き)

HMC インターフェース・タスクおよび 関連コマンド	ユーザー・ロール/ID			
	オペレーター (hmcoperator)	スーパー管理者 (hmcsuperadmin)	ビューアー (hmcviewer)	サービス担当員 (hmcservicerep)
35 ページの『再ビルド』 chsysstate	X	X		
33 ページの『パワー・マネージメント』 chpwrmgmt lspwrmgmt		X		
61 ページの『削除』 rmsyscfg	X	X		X
63 ページの『モビリティ』 lslparmigr migrlpar	X	X		X
64 ページの『プロファイルの管理』 chsyscfg lssyscfg mksyscfg rmsyscfg chsysstate	X	X		X
システム・プランの管理 cpsysplan rmsysplan		X		
システム・プランの作成 mksysplan		X		
システム・プランのデプロイ deploysysplan		X		
N_Port ログインの変更 chnportlogin	X	X		X
LPAR の RR 始動 lsrrstartlpar rrstartlpar	X	X		

表 7. システム管理タスク、コマンド、およびデフォルト・ユーザー・ロール (続き)

HMC インターフェース・タスクおよび 関連コマンド	ユーザー・ロール/ID			
	オペレーター (hmcoperator)	スーパー管理者 (hmcsuperadmin)	ビューアー (hmcviewer)	サービス担当員 (hmcservicerep)
LPAR の移行 migrdbg refdev	X	X		
プロファイル・データの作成 mkprofdata	X	X		
プロファイル・データの復元 migrcfg	X	X		
プロファイル・データの除去 rmprofdata	X	X		
Pmem CEC 構成の管理: プロファイル・データの初期化: プロファイル・データに復元 rstprofdata オプション "--retainpmemvolume" (hmcsuperadmin 専用のアクセス)	X	X		
Vios Admin Op: Virtual IO Server コマンド viosvrcmd オプション "--admin" (hmcsuperadmin および hmcoperator の専用のアクセス)	X	X		X
31 ページの『操作』	X	X	X	X
構成				
38 ページの『テンプレートから区画を作成』		X		
38 ページの『テンプレートからシステムをデプロイ』		X		
38 ページの『構成をテンプレートとして取り込む』		X		
CEC プロパティーの変更 chprimhmc	X	X		
トラステッド・システム鍵の変更 chtskey		X		

表 7. システム管理タスク、コマンド、およびデフォルト・ユーザー・ロール (続き)

HMC インターフェース・タスクおよび 関連コマンド	ユーザー・ロール/ID			
	オペレーター (hmcoperator)	スーパー管理者 (hmcsuperadmin)	ビューアー (hmcviewer)	サービス担当員 (hmcservicerep)
42 ページの『区画の作成』		X		
LPAR プロパティのリスト lsmigrdbg	X	X	X	X
LPAR のハイバネート lsrsdevsize	X	X		
N_Port ログインのリスト lsnportlogin	X	X		X
LS プロファイル・スペース lsprofspace	X	X	X	X
トラステッド・システム鍵のリスト lstkey	X	X	X	X
65 ページの『カスタム・グループの管理』	X	X		X
64 ページの『プロファイルの管理』 chsyscfg chsysstate lssyscfg mksyscfg rmsyscfg	X	X	X	X
ライセンス・キーの管理 chlickey	X	X		
使用状況データの管理 chlparutil	X	X		X
現在の構成の保管 65 ページの『現在の構成の保管』 mksyscfg	X	X		
ViewSPP lsmemdev	X	X	X	X
接続				

表 7. システム管理タスク、コマンド、およびデフォルト・ユーザー・ロール (続き)

HMC インターフェース・タスクおよび 関連コマンド	ユーザー・ロール/ID			
	オペレーター (hmcoperator)	スーパー管理者 (hmcsuperadmin)	ビューアー (hmcviewer)	サービス担当員 (hmcservicerep)
36 ページの『サービス・プロセッサ の状況』 lssysconn	X	X	X	X
37 ページの『接続のリセットまたは 除去』 rmsysconn	X	X		
接続の追加 mksysconn	X	X		
V Term のオープン mkvterm	X	X		X
V Term のクローズ rmvterm	X	X		X
37 ページの『他の HMC の切断』		X		
ハードウェア情報				
51 ページの『ハードウェア操作』	X	X	X	X
更新				
39 ページの『ライセンス内部コード の変更』 lslic updlic		X		X
39 ページの『システムの作動可能確 認』 updlic		X		X
38 ページの『システム情報の表示』 lslic		X		X
HMC の更新 updhmc lshmc		X		X
保守容易性				

表 7. システム管理タスク、コマンド、およびデフォルト・ユーザー・ロール (続き)

HMC インターフェース・タスクおよび 関連コマンド	ユーザー・ロール/ID			
	オペレーター (hmcoperator)	スーパー管理者 (hmcsuperadmin)	ビューアー (hmcviewer)	サービス担当員 (hmcservicerep)
65 ページの『サービス可能イベント・マネージャー』 chsvcevent lssvcevents		X		X
SNMP アラートの変更 chspsnmp	X	X		X
49 ページの『サービス可能イベントの作成』		X		X
66 ページの『参照コード・ログ』 lsrefcode	X	X	X	X
67 ページの『コントロール・パネル機能』 lssyscfg	X	X		
51 ページの『FRU の追加』		X		X
53 ページの『エンクロージャの追加』		X		X
52 ページの『FRU の交換』		X		X
52 ページの『FRU の除去』		X		X
53 ページの『エンクロージャの除去』		X		X
51 ページの『ユニットの電源オン/オフ』		X		X
50 ページの『ダンプの管理』 dump cpdump getdump lsdump startdump lsfru	X	X		X
50 ページの『VPD の収集』	X	X	X	X

表 7. システム管理タスク、コマンド、およびデフォルト・ユーザー・ロール (続き)

HMC インターフェース・タスクおよび 関連コマンド	ユーザー・ロール/ID			
	オペレーター (hmcoperator)	スーパー管理者 (hmcsuperadmin)	ビューアー (hmcviewer)	サービス担当員 (hmcservicerep)
51 ページの『 タイプ、モデル、フィーチャー 』		X		
53 ページの『 FSP フェイルオーバーのセットアップ 』 chsyscfg lssyscfg		X		
54 ページの『 FSP フェイルオーバーの開始 』 chsysstate		X		
CEC プロパティのリスト lsprimhmc	X	X	X	X
Capacity on Demand (CoD)				
CoD コードの入力 chcod		X		
ヒストリー・ログの表示 lscod	X	X	X	X
CEC プロパティの変更 chcomgmt	X	X		
CoD プールの管理: CoD の変更 chcodpool	X	X		
CoD の変更 mkcodpool		X		
VET コードの変更 chvet		X		
CoD 情報のリスト lscodpool	X	X	X	X
VET 情報のリスト lsvet	X	X	X	X
プロセッサ: キャパシティー設定の表示 lscod	X	X	X	X

表 7. システム管理タスク、コマンド、およびデフォルト・ユーザー・ロール (続き)

HMC インターフェース・タスクおよび 関連コマンド	ユーザー・ロール/ID			
	オペレーター (hmcoperator)	スーパー管理者 (hmcsuperadmin)	ビューアー (hmcviewer)	サービス担当員 (hmcservicerep)
プロセッサ CUoD: コード情報の表示 lscod	X	X	X	X
プロセッサ: On/Off CoD: 管理 chcod		X		
プロセッサ: On/Off CoD: キャパシティー設定の表示 lscod	X	X	X	X
プロセッサ: On/Off CoD: 請求情報の表示 lscod	X	X	X	X
プロセッサ: On/Off CoD: コード情報の表示 lscod	X	X	X	X
プロセッサ: Trial CoD: 停止 chcod		X		
プロセッサ: Trial CoD: キャパシティー設定の表示 lscod	X	X	X	X
プロセッサ: Trial CoD: コード情報の表示 lscod	X	X	X	X
プロセッサ: Reserve CoD: 管理 chcod		X		
プロセッサ: Reserve CoD: キャパシティー設定の表示 lscod	X	X	X	X
プロセッサ: Reserve CoD: コード情報の表示 lscod	X	X	X	X
プロセッサ: Reserve CoD: 共用プロセッサ使用状況の表示 lscod	X		X	X

表 7. システム管理タスク、コマンド、およびデフォルト・ユーザー・ロール (続き)

HMC インターフェース・タスクおよび 関連コマンド	ユーザー・ロール/ID			
	オペレーター (hmcoperator)	スーパー管理者 (hmcsuperadmin)	ビューアー (hmcviewer)	サービス担当員 (hmcservicerep)
PowerVM® (以前は、Advanced POWER® Virtualization と呼ばれてい た): 活動化コードの入力 chcod		X		
PowerVM: ヒストリー・ログの表示 lscod	X	X	X	X
PowerVM: コード情報の表示 lscod	X	X	X	X
エンタープライズ・イネーブルメント: 活動化コードの入力 chcod		X		
エンタープライズ・イネーブルメント: ヒストリー・ログの表示 lscod	X	X	X	X
エンタープライズ・イネーブルメント: コード情報の表示 lscod	X	X	X	X
その他の拡張機能: 活動化コードの入 力 chcod		X		
その他の拡張機能: ヒストリー・ログの 表示 lscod	X	X	X	X
その他の拡張機能: コード情報の表示 lscod	X	X	X	X
プロセッサ: 管理 chcod		X		
プロセッサ: キャパシティー設定の 表示 lscod	X	X	X	X
プロセッサ: コード情報の表示 lscod	X	X	X	X

表 7. システム管理タスク、コマンド、およびデフォルト・ユーザー・ロール (続き)

HMC インターフェース・タスクおよび 関連コマンド	ユーザー・ロール/ID			
	オペレーター (hmcoperator)	スーパー管理者 (hmcsuperadmin)	ビューアー (hmcviewer)	サービス担当員 (hmcservicerep)
メモリー: 管理 chcod		X		
メモリー: キャパシティー設定の表示 lscod	X	X	X	X
メモリー: コード情報の表示 lscod	X	X	X	X

以下の表は、コントロール・パネル機能タスク、コマンド、およびデフォルト・ユーザー・ロールを示します。

表 8. コントロール・パネル機能タスク、コマンド、およびユーザー・ロール

HMC インターフェース・タスク および関連コマンド	ユーザー・ロール/ID			
	オペレーター (hmcoperator)	スーパー管理者 (hmcsuperadmin)	ビューアー (hmcviewer)	サービス担当員 (hmcservicerep)
保守容易性				
(21) 専用サービス・ツールの活動化 chsysstate	X	X		
(65) リモート・サービスの使用不可化 chsysstate	X	X		
(66) リモート・サービスの使用可能化 chsysstate	X	X		
(67) ディスク装置 IOP のリセット/再ロード chsysstate	X	X		
(68) 並行保守電源オフ・ドメイン	X	X		
(69) 並行保守電源オン・ドメイン	X	X		
(70) IOP 制御記憶域のダンプ chsysstate	X	X		
(71) プロダクト・エンジニアリング・デバッグ・ツール pedbg				

表 8. コントロール・パネル機能タスク、コマンド、およびユーザー・ロール (続き)

HMC インターフェース・タスク および関連コマンド	ユーザー・ロール/ID			
	オペレーター (hmcoperator)	スーパー管理者 (hmcsuperadmin)	ビューアー (hmcviewer)	サービス担当員 (hmcservicerep)
(72) PE シェルへのアクセス権限 pesh	X	X	X	X

以下の表は、HMC UI タスクと関連していないコマンドについて説明し、各コマンドを実行できるデフォルトのユーザー・ロールを明示しています。

表 9. コマンド行タスク、関連コマンド、およびユーザー・ロール

コマンド行タスク	ユーザー・ロール/ID			
	オペレーター (hmcoperator)	スーパー管理者 (hmcsuperadmin)	ビューアー (hmcviewer)	サービス担当員 (hmcservicerep)
ローカルで認証された HMC ユーザーのパスワードを暗号化するのに HMC が使用する暗号化の変更、または HMC Web UI が使用できる暗号化の変更 chhmcencr		X		
ローカルで認証された HMC ユーザーのパスワードを暗号化するのに HMC が使用する暗号化のリスト、または HMC Web UI が使用できる暗号化のリスト chhmcfs	X	X	X	
HMC ファイル・システム内のスペースの解放 chhmcfs	X	X		
HMC ファイル・システム情報のリスト lshmcfs	X	X	X	X
HMC 上で取り外し可能メディアが作動可能かどうかのテスト ckmedia	X	X		X
リモート・サイトからの HMC アップグレード用の必要ファイルの取得 getupgfiles	X	X		X
HMC 上における画面取りの提供 hmcwin	X	X	X	X

表 9. コマンド行タスク、関連コマンド、およびユーザー・ロール (続き)

コマンド行タスク	ユーザー・ロール/ID			
	オペレーター (hmcoperator)	スーパー管理者 (hmcsuperadmin)	ビューアー (hmcviewer)	サービス担当員 (hmcservicerep)
SSH コマンド使用状況のログ記録 logssh	X	X	X	X
管理対象システム上における区画構成データの消去またはダンプ lpcfgop		X		
管理対象フレーム、または管理対象フレーム内にあるシステムの環境情報のリスト lshwinfo	X	X	X	X
管理対象フレームに対するロックを所有する HMC のリスト lslock	X	X	X	X
管理対象フレームに対する HMC ロックの強制的解放 rmlock		X		
HMC における使用に対応可能なストレージ・メディア・デバイスのリスト lsmediadev	X	X	X	X
SSH 認証鍵の管理 mkauthkeys	X	X	X	X
HMC サブシステムおよびシステム・リソースのモニター monhmc	X	X	X	X
管理対象システムについて収集された使用状況データの、HMC からの除去 rmlparutil	X	X		X
制限モードの HMC 上でユーザーがテキスト・ファイルを編集できるようにする rnvi	X	X	X	X

表 9. コマンド行タスク、関連コマンド、およびユーザー・ロール (続き)

コマンド行タスク	ユーザー・ロール/ID			
	オペレーター (hmcoperator)	スーパー管理者 (hmcsuperadmin)	ビューアー (hmcviewer)	サービス担当員 (hmcservicerep)
DLPAR 障害後の、ハードウェア・リソースの復元 rsthwres		X		
HMC 上でのアップグレード・データの復元 rstupgdata	X	X		X
HMC からリモート・システムへのファイルの転送 sendfile	X	X	X	X
chsvc	X	X		X
lssvc	X	X	X	X
chstat	X	X		X
lsstat	X	X	X	X
chpwdpolicy		X		
lspwdpolicy	X	X	X	X
mkpwdpolicy		X		
rmpwdpolicy		X		
expdata		X		

セッション処理

ハードウェア管理コンソール (HMC) におけるセッションの制約事項について説明します。

セッションの制限事項

HMC は切断されたセッションをサポートしません。セッション・ログオフおよびセッション切断はどちらも、セッション・ログオフと見なされます。つまり、同じセッションに再接続して、前のセッションで開始されたタスク (単数または複数) を再開することはできません。HMC からログインするたびに、新しいセッションが作成されます。

1. HMC インターフェースから 長期間実行するタスクを開始してから、そのセッションからログオフした場合、その長期間実行するタスクはバックグラウンドで実行し続けます。ただし、再度ログインすると、新しいセッションが作成され、「タスクの進行状況」パネル (前のタスクの進行状況を追跡する上で役立ちます) は使用できなくなります。このシナリオでは、前のセッションで開始されたタスクの進行状況を調べる必要がある場合、個別のコマンド行インターフェース (CLI) コマンドの実行、管理対象リソースの状態の確認、またはコンソール・イベント・ログの確認を行えます。

注: 長期間実行するタスクの例として、以下のタスクがあります。

サーバーのためのシステム 管理:

- システム・プランのデプロイ
- コード更新
- ハードウェア - ホット修復/アップグレードの準備

区画のためのシステム 管理

- テラバイト順の大きい単位での DLPAR メモリー
- Live Partition Mobility (LPM)
- 中断または再開

HMC 管理:

- 管理コンソール・データのバックアップ
 - 管理コンソール・データのリストア
 - アップグレード・データの保管
2. タイムアウト時間の検査設定に指定されている時間内に再認証できない場合、現在のセッションから自動的にログオフされます。
 3. アイドル・タイムアウトのユーザー・プロパティ・タスクは機能しません。HMC インターフェースでは、アイドル・タイムアウト設定にデフォルト値 **0** を使用します。この設定に別の値を設定した場合、その設定は無視されます。

注: セッション、アイドル、およびタイムアウト時間の検査の各属性はユーザーに代わって設定され、同じ HMC 上でもユーザーごとに異なる可能性があります。

管理対象システムの「バージョン不一致」状態

「バージョン不一致」状態は、同じサーバーを管理する冗長ハードウェア管理コンソール (HMC) またはデュアルハードウェア管理コンソール (HMC) のバージョンおよびリリース・レベルが異なる場合に発生することがあります。

「バージョン不一致」状態は、以下のどの理由でも起きることがあります。

- FSP のファームウェアと HMC のバージョンが適合しない。
- HMC バージョン 7.7.8 以降を、より新しいバージョンの HMC で管理されたサーバーに接続する。
- HMC バージョン 7.7.8 以降が下位バージョンの HMC で管理されたサーバーに接続し、データを HMC バージョン 7.7.8 以降にアップグレードするためのスペースが十分ではない。
- ハイパーバイザーまたはサーバーの製品またはモデルが、このバージョンの HMC によってサポートされていない。

「バージョン不一致」状態からリカバリーするには、表示される参照コードに応じて、以下の中から該当する処理を選択してください。

• 保管域バージョン不一致

HMC バージョン 7.7.8 以降は、新規の「接続エラー」状態と参照コードを通知して、より新しいレベルの構成を持つサーバーを管理する試みをブロックします。HMC バージョン 7.7.8 以降では、構成形式が更新されたより新しいバージョンの HMC で管理されたサーバーに接続する場合、HMC により、参照コード「保管域バージョン不一致」が付いた「バージョン不一致」の接続エラーが報告されます。このエラーにより構成が誤って破壊されることが防止されます。

下位バージョンの HMC を継続したい場合、操作を続ける前に、下位バージョンの HMC でサーバーを初期化する必要があります。

• プロファイル・データ保管域が満杯 (Profile Data Save Area is full)

HMC は、各管理対象サーバー上でストレージ域を使用して、サーバー構成、主として PowerVM パーティション・プロファイルを保管します。HMC 7.8.0 以降では、区画ごとに別のプロファイル (多くは非表示) が追加され、ストレージ域の使用量が増加します。既に多くのプロファイルを含んでいるサーバーでは、HMC バージョン 7.8.0 以降を適切に実行できるだけのスペースが十分ではないことがあります。

HMC バージョン 7.8.0 以降は、このストレージ域に十分なスペースがあるかが検査され、スペースが十分でない場合は、「バージョン不一致」の接続状態および「プロファイル・データ保管域が満杯 (Profile Data Save Area is full)」の参照コードで、接続プロセスが停止します。

- **0000-0000-00000000 の接続 (サポートされないハイパーバイザー) (Connecting 0000-0000-00000000 (Unsupported Hypervisor))**

サーバーが PowerVM 以外のハイパーバイザー用に構成されている場合、「バージョン不一致」の接続状態および「**0000-0000-00000000 の接続 (サポートされないハイパーバイザー) (Connecting 0000-0000-00000000 (Unsupported Hypervisor))**」という参照コードが返されます。

この状態から回復するには、まず最初に、「バージョン不一致」が示されているサーバーを選択して ASM を開始し、「操作」を選択してから、「拡張システム管理 (ASM) の起動」を選択してください。

複数のハイパーバイザーをサポートするモデルでは、「システム構成」を選択し、次に「ハイパーバイザー構成」を選択すると、ASM 内のハイパーバイザー・モード設定が示されます。ハイパーバイザー・モードでは、PowerVM または OPAL のいずれかの設定が示されます。

OPAL が必要な構成である場合は、「接続」を選択し、次に「接続のリセットまたは除去」を選択して、HMC からこの接続を除去する必要があります。続いて、「接続の除去」を選択して、「了解」をクリックします。

注: OPAL ハイパーバイザーは HMC ではサポートされていません。

PowerVM が必要な構成である場合は、ハイパーバイザー・モードのメニューから「PowerVM」を選択して、「続行」をクリックします。

注: 設定を変更できるのは、サーバーの電源がオフになっている場合だけです。サーバーの電源をオフにするには、「電源/再始動制御」を選択してから、「システムの電源オン/オフ」を選択してください。「設定を保存して電源オフ」をクリックします。

- **接続は許可されない (Connection not allowed)**

FSP ファームウェアと HMC バージョンが矛盾する場合、「バージョン不一致」の状態および「**0009-0008-00000000 の接続は許可されない (Connection not allowed 0009-0008-00000000)**」という参照コードが返されます。

この状態から回復するには、管理対象サーバー・モデルをサポートする HMC バージョンをインストールしてください。

「バージョン不一致」状態の修正について詳しくは、『バージョン不一致』を参照してください。

システム管理 (サーバー)

「システム管理」は、サーバー、論理区画、およびフレームを管理するタスクを表示します。これらのタスクを使用して、サーバーのセットアップおよび構成を行い、現在の状態を表示し、トラブルシューティングを行い、さらに解決策を適用します。

これらのタスクは、管理対象システムが選択されたときにリストされます。メニュー・ポッドにリストされるタスクは、作業域で選択を行うと変わります。

システム・コンテンツ・ペイン

管理コンソールに接続されているすべてのシステムの状態、正常性、およびキャパシティー情報を表示およびモニターします。

ウィンドウの中央部分にあるコンテンツ・ペインには、すべての使用可能なシステムと、各サーバーの関連情報が表示されます。情報を表ビューで表示するかギャラリー・ビューで表示するかを選択できます。

各システムについて、現在のシステムの状態、使用中の中央演算処理装置 (CPU) の数、使用可能な CPU の数、使用中のランダム・アクセス・メモリー (RAM) の量、使用可能な RAM の量が表示されます。さらに、表形式のビューを選択した場合は、表の右上隅にあるドロップダウン矢印を選択することで、表示される情報をフィルタリングすることができます。表に表示したいフィールドに対応するチェック・ボックスを選択します。HMC バージョン 9.1.930 を使用している場合は、「すべてのシステム」表で、活動化されて

いるファームウェア・レベルと据え置きされているファームウェア・レベルに関する情報を表示することもできます。

「**属性**」アイコンをクリックして、以下の情報を表示することができます。

- 現在の状態
- 参照コード
- マシン・タイプ
- シリアル 番号
- システムのロケーション
- ファームウェア・レベル
- グループ・タグ
- アテンション LED

「**capacity**」アイコンをクリックして、以下の情報を表示することができます。

- 収集の日付。
- プロセッサ使用状況 (取り付け済み、活動化済み、使用可能、平均、およびピーク)。棒グラフと数値によって、平均使用率 (「平均」を「活動化済み」で除算) がパーセンテージで示されます。棒グラフのしきい値ラインは、ピークしきい値 (「ピーク」を「活動化済み」で除算) を示します。値がしきい値を超えると、棒グラフの書式が破線に変更されます。
- メモリー割り当て (取り付け済み、活動化済み、使用可能、平均、およびピーク)。棒グラフと数値によって、平均使用率 (「平均」を「活動化済み」で除算) がパーセンテージで示されます。棒グラフのしきい値ラインは、ピークしきい値 (「ピーク」を「活動化済み」で除算) を示します。値がしきい値を超えると、棒グラフの書式が破線に変更されます。
- ネットワーク I/O 使用状況 (1 秒当たりの送信および受信キロバイト数、および 1 秒当たりのパケット数)。棒グラフと数値によって、平均使用率 ((平均転送バイト数をアダプター数で除算した値) を最大転送バイト数で除算) がパーセンテージで示されます。棒グラフのしきい値ラインは、上限しきい値 (最大転送バイト数) を示します。値がしきい値を超えると、棒グラフの書式が破線に変更されます。
- ストレージ I/O 使用状況 (1 秒当たりの書き込みおよび読み取り情報量 (キロバイト数))。棒グラフと数値によって、平均使用率 ((平均転送バイト数をアダプター数で除算した値) を最大転送バイト数で除算) がパーセンテージで示されます。棒グラフのしきい値ラインは、上限しきい値 (最大転送バイト数) を示します。値がしきい値を超えると、棒グラフの書式が破線に変更されます。
- データ収集。

「**すべてのシステム**」ウィンドウでシステム上にカーソルを移動して、システム・モデルの説明を表示することもできます。

操作

「**操作**」には、管理対象システムを操作するためのタスクが含まれています。

電源オフ

管理対象システムをシャットダウンします。管理対象システムの電源をオフにすると、システムの電源を再度オンにするまで、すべての区画は使用不可になります。

管理対象システムを電源オフする前に、すべての論理区画がシャットダウンされていて、その状態が「実行中 (Running)」から「活動化されていない (Not Activated)」に変化したことを確認してください。論理区画のシャットダウンについて詳しくは、[60 ページの『シャットダウン』](#)を参照してください。

管理対象システムの電源をオフする前に、その管理対象システムのすべての論理区画をシャットダウンしなければ、管理対象システムが、管理対象システム自体の電源オフの前に、各論理区画をシャットダウンします。これによって、論理区画の応答が遅い場合は特に、管理対象システムの電源オフにかなりの遅れが生じる場合があります。さらに、論理区画が異常にシャットダウンされることがあり、この場合は論理区画を再度活動化したとき、データが失われたり、さらに遅れる可能性があります。

以下のオプションから選択してください。

通常の電源オフ

「通常の電源オフ」モードは、制御された方法でシステムの操作をシャットダウンします。シャットダウンの間、アクティブなジョブで実行されているプログラムは、クリーンアップ (ジョブ終了処理) を実行できます。

高速電源オフ

「高速電源オフ」モードは、すべてのアクティブなジョブを直ちに停止してシステムをシャットダウンします。それらのジョブで実行中のプログラムは、ジョブのクリーンアップを行うことができません。このオプションは、緊急またはクリティカルな状態であるという理由でシステムのシャットダウンが必要な場合に使用してください。

電源オン

「電源オン」タスクを使用して、管理対象システムを開始します。

以下のオプションから選択して、管理対象システムを電源オンします。

通常 (Normal): このオプションは、HMC が区画開始ポリシーの現行設定を使用して管理対象システムの電源オン方法を決定することを指定する場合に選択します。現行設定は、以下の値のいずれかです。

- **常に自動開始 (Auto-Start Always):** このオプションは、管理対象システムの電源がオンになると HMC が自動的に論理区画を電源オンすることを指定します。管理対象システムの電源オンがユーザー・アクションの結果である場合、HMC は自動始動用に構成されたすべての区画を開始します。管理対象システムの電源が自動リカバリー・プロセスの結果オンになった場合、HMC は、システムが電源オフされたときに実行中だった論理区画のみを開始します。このオプションは常に選択可能です。
- **区画スタンバイで停止:** このオプションは、管理対象システムの電源オン後の論理区画始動がスタンバイ・モードであり、管理対象システムの電源がオンになったときに HMC がどの論理区画も始動しないことを指定します。管理対象システムの電源が自動リカバリー・プロセスの結果オンになり、しかも論理区画を始動するのに HMC が使用される場合、HMC は、システムが電源オフされたときに実行中だったすべての論理区画を始動します。このオプションは、管理対象システムのファームウェアが拡張 IPL 機能をサポートしていない場合にのみ選択可能です。
- **自動リカバリーの場合に自動開始 (Auto-Start for Auto-Recovery):** このオプションは、自動リカバリー・プロセスの結果として管理対象システムが電源オンになった後でのみ、HMC が論理区画を自動的に電源オンすることを指定します。このオプションは、管理対象システムのファームウェアが拡張 IPL 機能をサポートしている場合にのみ選択可能です。
- **ユーザーによる開始:** このオプションは、管理対象システムの電源がオンになったときに HMC がいかなる論理区画も始動しないように指定します。管理対象システム上の論理区画を、HMC を使用して手動で開始する必要があります。このオプションは、管理対象システムのファームウェアが拡張 IPL 機能をサポートしている場合にのみ選択可能です。

管理対象システムに対する「属性」タスクの「電源オン・パラメーター」ページから区画開始ポリシーを設定できます。

システム・プロファイル (System profile): この電源オン・オプションを選択すると、事前定義済みのシステム・プロファイルに基づいて HMC がシステムおよびその論理区画を電源オンするよう指定されます。この電源オン・オプションを選択する場合は、HMC が管理対象システム上の論理区画を活動化するとき使用するパーティション・プロファイルを選択する必要があります。

ハードウェア・ディスカバリー (Hardware Discovery): この電源オン・オプションを選択すると、管理対象システムの電源オン時に HMC がハードウェア・ディスカバリー・プロセスを実行するよう指定されます。ハードウェア・ディスカバリー・プロセスは、すべての I/O デバイス (特に、現在パーティションに割り当てられていないデバイス) に関する情報をキャプチャーします。管理対象システムについてハードウェア・ディスカバリーの電源オン・オプションを選択した場合、その管理対象システムは電源オンされたとき、ハードウェア・ディスカバリーを実行する特別なモードになります。ハードウェア・ディスカバリー・プロセスが完了すると、区画は電源オフの状態、システムは「稼働中」状態になります。ハードウェア・ディスカバリー・プロセスは、管理対象システム上のキャッシュにハードウェア・インベントリを記録します。収集された情報は、入出力装置用にデータを表示する場合、または管理対象システムに基づいてシステム・プランを作成する場合に使用することができます。このオプションは、システムがハードウェア・ディスカバリー・プロセスを使用して管理対象システム用の入出力ハードウェア・インベントリを取り込むことができる場合にのみ、選択可能です。

パワー・マネージメント

省電力モードを有効にすることにより、管理対象システムのプロセッサの電力消費量を削減することができます。

このタスクについて

省電力モードを有効にするには、以下の手順を完了します。

手順



1. ナビゲーション領域で、リソース・アイコン  をクリックしてから、「すべてのシステム」を選択します。
2. 省電力モードを使用可能にしたいサーバーを選択し、「アクション」 > 「すべてのアクションの表示」をクリックします。
3. 「操作」で「パワー・マネージメント」を選択します。
4. 以下の省電力モードのオプションのいずれかを選択します。
 - **すべてのモードを無効にする:** 省電力モードを無効にします。プロセッサのクロック周波数は公称値に設定され、システムが使用する電力は公称レベルのままです。
 - **静的モードを有効にする:** プロセッサのクロック周波数と電圧を固定値まで下げることによって、電力消費量を低減します。このオプションは、予測可能なパフォーマンスを実現する一方で、システムの電力消費量も削減します。
 - **動的パフォーマンス・モードを有効にする:** プロセッサの周波数が、プロセッサ使用に基づいて変化するようになります。プロセッサ使用中程度または高い間、プロセッサ周波数は、最大許容値に設定されます。この値は、公称周波数より大きい場合があります。また、プロセッサ使用が低い間、周波数は、公称周波数より小さい値に設定されます。
 - **最大パフォーマンス・モードを有効にする:** プロセッサ周波数が、ユーザーが指定できる固定値に設定されます。システムのプロセッサ周波数および電力消費量の最大限度を設定することができます。

注: いずれかの省電力モードを使用可能にすると、プロセッサの周波数、プロセッサ使用、電力消費量、およびパフォーマンスが変化します。

操作のスケジュール

オペレーターの介入なしで、管理対象システム上で実行する特定の操作のスケジュールを作成します。

システム操作の自動処理、遅延処理、または反復処理が必要な状況では、スケジュール操作が便利です。スケジュール操作は、指定した時刻に、オペレーターが操作の実行に携わることなく開始します。スケジュールには、1回の操作または複数回の繰り返しを設定できます。

例えば、管理対象システムの電源オン/オフ操作をスケジュールできます。

「スケジュール操作」タスクは、各操作について次の情報を表示します。

- 操作の対象になるプロセッサ
- スケジュールされている日付
- スケジュールされている時刻
- 操作
- 残されている繰り返し回数

「スケジュール操作」ウィンドウでは、以下のタスクを実行できます。

- 操作を後で実行するようスケジュールします。
- 操作を定期的な間隔で繰り返し実行するように定義します。
- スケジュール操作を削除します。

- 現在スケジュールされている操作の詳細を表示します。
- 指定した時刻範囲内にスケジュールされている操作を表示します。
- スケジュールされている操作を、日付、操作、または管理対象システム別にソートします。

ある操作が一度実行されるようにスケジュールするか、またはそれが繰り返し実行されるようにスケジュールすることができます。操作が実行される時刻および日付を指定する必要があります。操作を繰り返し実行させたい場合、以下のオプションを選択する必要があります。

- 操作を実行する曜日 (任意)
- 操作の実行間隔または時刻 (必須)
- 繰り返しの合計回数 (必須)

管理対象システムについてスケジュール可能な操作には、以下のものがあります。

システム・プロファイルに対する活動化

選択したシステム・プロファイルの活動化をスケジュールするために、選択したシステム上での操作をスケジュールします。

プロファイル・データのバックアップ

管理対象システムのプロファイル・データをバックアップする操作をスケジュールします。

管理対象システムの電源オフ

1つの管理対象システムに一定間隔でシステム電源オフにする操作をスケジュールします。

管理対象システムの電源オン

1つの管理対象システムに一定間隔でシステム電源オンにする操作をスケジュールします。

Utility CoD プロセッサを管理する

ご使用の Utility CoD プロセッサの使用法を管理するための操作をスケジュールします。

Utility CoD プロセッサの分使用限度の管理

Utility CoD プロセッサ使用量の限度を作成します。

共用プロセッサ・プールの変更

共用プロセッサ・プールを変更するための操作をスケジュールします。

別のプールに区画を移動

別のプロセッサ・プールに区画を移動させるための操作をスケジュールします。

管理対象システムの省電力モードを変更

管理対象システムの省電力モードを変更するための操作をスケジュールします。

動的プラットフォーム最適化のモニター/実行

動的プラットフォーム最適化を実行したり、ユーザーに電子メールの通知アラートを送信したりするための操作をスケジュールします。

管理対象システム上の操作をスケジュールするには、以下のステップを完了します。

1. ナビゲーション領域で、リソース・アイコン  をクリックしてから、「すべてのシステム」を選択します。
2. 1つ以上の管理対象システムを選択し、「アクション」 > 「操作のスケジュール」をクリックします。
3. 「操作のスケジュール」ウィンドウから、メニューバーの「オプション」をクリックし、オプションの次のレベルを表示します。
 - スケジュール操作を追加するには、「オプション」をクリックしてから「新規」をクリックします。
 - スケジュール操作を削除するには、削除する操作を選択して「オプション」を選択してから「削除」をクリックします。
 - 選択したオブジェクトについて、スケジュール操作のリストを現在のスケジュールで更新するには、「オプション」を選択してから「最新表示」をクリックします。
 - スケジュール操作を表示するには、表示する操作を選択して「表示」を選択してから「スケジュールの詳細」をクリックします。

- スケジュール操作の時間を変更するには、変更する操作を選択して「表示」を選択してから「新しい時間範囲...」をクリックします。
- スケジュール操作をソートするには、「ソート」を選択してから表示されるソート・カテゴリのいずれかをクリックします。

4. ウィンドウを閉じるには、「オプション」をクリックしてから「終了」をクリックします。

ASM インターフェースの起動

ハードウェア管理コンソール (HMC) は、選択したシステムの Advanced System Management Interface (ASMI) に直接接続することができます。

ASMI はサービス・プロセッサとのインターフェースで、これにより電源の自動再始動などのサーバーの動作を管理したり、エラー・ログや重要プロダクト・データなどのサーバーに関する情報を表示したりできます。

Advanced System Management Interface に接続するには、以下の手順を実行します。



1. ナビゲーション領域で、リソース・アイコン  をクリックしてから、「すべてのシステム」を選択します。
2. コンテンツ領域で、1 つ以上の管理対象システムを選択し、「アクション」 > 「すべてのアクションの表示」 > 「拡張システム管理 (ASM) の起動」をクリックします。

再ビルド

管理対象システムから構成情報を抽出し、ハードウェア管理コンソール (HMC) 上に情報を再ビルドすることができます。

このタスクによって、実行中のサーバーの操作が中断されることはありません。

管理対象システムを再ビルドすると、その管理対象システムに関して HMC 上にある情報が更新されます。管理対象システムの再ビルドは、管理対象システムの状態が Incomplete (不完全) である場合に有効です。「Incomplete」の状態とは、管理対象システムの論理区画、プロファイル、またはリソースから、HMC が完全な情報を収集できない状態を意味します。

管理対象システムの再ビルドは、HMC ウィンドウを最新表示するのとは異なります。管理対象システムが再ビルドされると、HMC は管理対象システムから情報を抽出します。HMC が管理対象システムを再ビルドしている間は、他のタスクを開始できません。このプロセスには数分かかることがあります。

パスワードの変更

選択した管理対象システムに対するハードウェア管理コンソール (HMC) アクセス・パスワードを変更します。

パスワードを変更したら、この管理対象システムにアクセスする他のすべての HMC について HMC アクセス・パスワードを更新する必要があります。

現在のパスワードを入力してから、新しいパスワードを入力し、検証のために新しいパスワードを再度入力してください。

アテンション LED

管理対象システム上でのシステム・アテンション LED 情報の表示、特定の LED の点灯によるシステム・コンポーネントの識別、およびすべての LED のテストを行います。

システムは、エンクロージャーや現場交換可能ユニット (FRU) など、システム内のさまざまなコンポーネントを識別するのに役立ついくつかの LED を備えています。この理由から、これらの LED は識別 LED と呼ばれます。個々の LED は、コンポーネント上またはその近くにあります。LED は、コンポーネント自身かまたはコンポーネントのキャリア (例えば、メモリー・カード、ファン、メモリー・モジュール、またはプロセッサ) に付いています。LED は緑色またはオレンジ色です。緑色の LED は、次のいずれかの状態を示します。

- 電源が入っている
- リンク上でアクティビティあり (システムが情報の送信または受信を行っている)

オレンジ色の LED は障害または識別状態を示します。システムまたはシステム上のいずれかのコンポーネントのオレンジ色の LED が点灯または明滅している場合は、問題を識別し、システムを正常な状態に戻すための適切な処置を行ってください。

ユーザーは、以下のタイプの識別 LED を活動化または非活動化することができます。

エンクロージャの識別 LED

特定のドロワー (エンクロージャ) にアダプターを追加する場合、ドロワーのマシン・タイプ、モデル、およびシリアル番号 (MTMS) を知っている必要があります。新規アダプターを必要とするドロワー用の正しい MTMS を持っているかどうかを調べるには、ドロワーの LED を活動化して、MTMS が新規アダプターを必要とするドロワーに対応しているかどうかを確認することができます。

指定したエンクロージャに関連する FRU の識別 LED

特定の入出力アダプターにケーブルを接続する場合、現場交換可能ユニット (FRU) であるアダプターの LED を活動化して、ケーブルの接続場所を物理的に確認することができます。このステップは、オープン・ポートを持つアダプターがいくつかある場合に特に役立ちます。

システム・アテンション LED または論理区画 LED を非活動化することができます。例えば、問題が優先度の高いものでないと判別し、その問題を後で修復する場合があります。ただし、別の問題が発生した場合はアラートを受け取りたいので、システム・アテンション LED を非活動化して、別の問題が発生したときに再度活動化できるようにする必要があります。

以下のオプションから選択してください。

アテンション LED をオフにする

このタスクから、システム・アテンション LED を非活動化することができます。

アテンション LED の識別

選択したエンクロージャに含まれるすべてのロケーション・コードの識別 LED の現在の状態を表示します。このタスクでは、該当するボタンを選択することによって、操作の対象として単一のロケーション・コードまたは複数のロケーション・コードを選択して、1 つ以上の LED を活動化したり非活動化したりすることができます。

アテンション LED のテスト

選択したシステムに対して LED ランプ・テストを開始します。数分間ですべての LED が活動化されます。

接続

サービス・プロセッサまたはフレームへのハードウェア管理コンソール (HMC) 接続状況の表示、これらの接続のリセット、選択した管理対象システムへの他の HMC の接続、または別の HMC の切断を行うことができます。

作業域で管理対象システムを選択した場合、以下のタスクがその管理対象システムに関連付けられます。フレームを選択すると、タスクはそのフレームに関係します。

サービス・プロセッサの状況

管理対象システム上のサービス・プロセッサへのハードウェア管理コンソール (HMC) 接続の状況に関する情報を表示します。

このタスクについて

管理対象システムで、サービス・プロセッサへのサービス・プロセッサ接続状況を表示するには、以下の手順を完了します。

手順



1. ナビゲーション領域で、リソース・アイコン をクリックしてから、「すべてのシステム」を選択します。
2. サービス・プロセッサの接続状況を表示したいサーバーを選択し、「アクション」 > 「すべてのアクションの表示」 > 「サービス・プロセッサの状況」をクリックします。

接続のリセットまたは除去

ハードウェア管理コンソール (HMC) インターフェースから、管理対象システムのリセットまたは除去を行います。

このタスクについて

接続をリセットまたは除去するには、次の手順を完了します。

手順



1. ナビゲーション領域で、リソース・アイコン をクリックしてから、「すべてのシステム」を選択します。
2. リセットまたは除去したいサーバーを選択し、「アクション」 > 「システム接続のリセットまたは除去」をクリックします。
3. 「接続のリセット」または「接続の除去」からオプションの 1 つを選択し、「OK」をクリックします。

他の HMC の切断

選択したハードウェア管理コンソール (HMC) と管理対象サーバー間の接続を切断できます。

このタスクについて

別の HMC を切断するには、以下の手順を実行します。

手順



1. ナビゲーション領域で、リソース・アイコン をクリックしてから、「すべてのシステム」を選択します。
2. 別の管理コンソールを切断したいサーバーを選択し、「アクション」 > 「すべてのアクションの表示」 > 「他の HMC の切断」をクリックします。
3. リストから HMC を選択し、「OK」をクリックする。

システムのテンプレート

システムのテンプレートにはリソース (システム・プロパティ、共有プロセッサ・プール、予約ストレージ・プール、共用メモリー・プール、ホスト・イーサネット・アダプター、SR-IOV アダプターなど) に関する構成の詳細が含まれています。個別タスクを使用して事前に構成したシステム設定の多くは、「**テンプレートからシステムをデプロイ**」ウィザードから使用可能です。例えば、ウィザードを使用してシステム・テンプレートからシステムをデプロイする場合、バーチャル I/O サーバー、仮想ネットワーク・ブリッジ、および仮想ストレージ設定を構成できます。

テンプレート・ライブラリーには、定義済みのシステム・テンプレートが収容されており、テンプレートには共通の使用シナリオに基づいた構成設定が含まれています。定義済みのシステム・テンプレートは、すぐに利用することができます。

また、ユーザーの環境に特有の構成設定を組み込んだカスタムのシステム・テンプレートを作成することもできます。カスタム・テンプレートを作成するには、定義済みテンプレートをコピーし、ユーザーの要件に合わせて変更します。また、既存のシステム構成を取り込んで、その詳細をテンプレートに保存することができます。その後で、そのテンプレートを同じ構成を必要とする他のシステムにデプロイできます。

テンプレートからシステムをデプロイ

ハードウェア管理コンソール (HMC) のテンプレート・ライブラリー内で使用可能なシステム・テンプレートを使用して、システムをデプロイできます。「テンプレートからシステムをデプロイ (Deploy System from Template)」ウィザードを使用することで、選択したシステムのデプロイメントの完了に必要な、ターゲット・システム固有の情報が提供されます。

テンプレートから区画を作成

ハードウェア管理コンソール (HMC) のテンプレート・ライブラリー内で使用可能な区画テンプレートを使用して、区画を作成できます。「テンプレートから区画を作成 (Create a Partition from Template)」ウィザードにより、デプロイメント・プロセスから構成手順までのガイドが提供されます。

構成をテンプレートとして取り込む

ハードウェア管理コンソール (HMC) を使用して、稼働中サーバーの構成詳細を取り込み、その情報をカスタムのシステム・テンプレートとして保存することができます。この機能は、同一構成を持つ複数のサーバーをデプロイする場合に役立ちます。定義済みテンプレートを使用する場合、この作業を完了する必要はありません。

構成をテンプレートとして取り込むには、以下のステップを実行します。

1. ナビゲーション領域で、リソース・アイコン  をクリックしてから、「すべてのシステム」を選択します。
2. システム情報を表示したいサーバーを選択し、「アクション」 > 「すべてのアクションの表示」をクリックします。
3. 「構成を物理 I/O のあるテンプレートとして取り込む (Capture Configuration as Template with Physical I/O)」または「構成を物理 I/O のないテンプレートとして取り込む (Capture Configuration as Template without Physical I/O)」をクリックします。
4. テンプレート名と説明を入力してから、「OK」をクリックします。

テンプレートとしての構成の取り込みに関する追加情報が必要な場合は、オンライン・ヘルプを使用してください。

更新

システム情報の表示、ご使用のハードウェア管理コンソール (HMC) での更新の管理、またはシステムの作動可能確認を行うためのタスクを表示します。

システム情報の表示

ハードウェア管理コンソール (HMC) から、選択したシステムに関する情報を表示します。

ネットワーク・トポロジを表示するには、以下の手順を実行します。

1. ナビゲーション領域で、リソース・アイコン  をクリックしてから、「すべてのシステム」を選択します。
2. システム情報を表示したいサーバーを選択し、「アクション」 > 「更新」 > 「システム情報の表示」をクリックします。
3. リストから LIC リポジトリを選択し、「OK」をクリックします。
4. このタスクを終了したら、「閉じる」をクリックします。

HMC のシステム情報の表示について詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

ライセンス内部コードの変更

ハードウェア管理コンソール (HMC) を使用して、管理対象システムのライセンス 内部コードを変更します。現行リリースのライセンス 内部コードを変更したり、新規リリースに変更したりすることができます。

ライセンス 内部コードを変更するには、以下の手順を完了します。



1. ナビゲーション領域で、リソース・アイコン をクリックしてから、「すべてのシステム」を選択します。
2. システム情報を表示したいサーバーを選択し、「アクション」 > 「更新」をクリックします。
3. 「現行リリースのライセンス 内部コードの変更」 > または 「ライセンス 内部コードを新規リリースに変更」 > を選択します。

注：「**ライセンス 内部コードの変更の開始**」ウィザードをクリックして、管理対象システム、電源、および I/O のライセンス 内部コード (LIC) のガイド付き更新を開始します。「**システム情報の表示**」をクリックして、検索可能レベルを含む現行 LIC レベルを検査します。追加のオプションと追加のターゲット選択項目を指定して管理対象システムを更新し、LIC を動作させるには、「**拡張機能の選択**」をクリックします。

4. リストからアクションを選択して、「了解」をクリックします。
5. このタスクを完了したら、「閉じる」をクリックします。

HMC のライセンス 内部コードの変更について詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

システムの作動可能確認

ハードウェア管理コンソール (HMC) から、選択したシステムのライセンス 内部コードの作動可能性を確認します。

システムの作動可能確認を行うには、以下の手順を実行します。



1. ナビゲーション領域で、リソース・アイコン をクリックしてから、「すべてのシステム」を選択します。
2. システム情報を表示したいサーバーを選択し、「アクション」 > 「更新」 > 「システムの作動可能確認」をクリックします。
3. このタスクが完了したら、「了解」をクリックします。

HMC のシステムの作動可能確認について詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

SR-IOV ファームウェア更新

ご使用のハードウェア管理コンソール (HMC) 上の SR-IOV アダプターのドライバー・ファームウェアを更新します。

注：アダプターは共用モードになっている必要があります。

SR-IOV アダプターのファームウェアを更新するには、以下のステップを完了します。



1. ナビゲーション領域で、リソース・アイコン をクリックしてから、「すべてのシステム」を選択します。
2. システム情報を表示したいサーバーを選択し、「アクション」 > 「更新」 > 「**SR-IOV ファームウェア更新**」をクリックします。

3. アダプター (単数または複数) を選択して右クリックし、コンテキスト・メニューを取得します。

4. 開始するファームウェア更新のタイプを選択します。

注: アダプター・ドライバー・ファームウェアを更新するか、アダプター・ドライバーとアダプター・ファームウェアの両方を更新することができます。アダプターまたはアダプター・ドライバー・ファームウェアの更新操作中に、アダプター上の構成済み論理ポートでネットワーク・トラフィックの一時的な切断が発生する場合があります。各アダプターの更新は、2分から5分かかる可能性があります。更新は、順次に実行されます。

5. このタスクを終了したら、「閉じる」をクリックします。

SR-IOV アダプターのドライバーまたはファームウェアを更新するための詳細情報が必要な場合は、オンライン・ヘルプを使用してください。

レガシー

ハードウェア管理コンソール (HMC) 上で選択可能な「**レガシー (legacy)**」タスクを確認できます。

作業域で管理対象システムを選択した場合、以下の「**レガシー**」タスクがその管理対象システムに関連付けられます。

区画可用性の優先順位

このタスクを使用して、この管理対象システム上の論理区画について、それぞれの区画可用性優先順位を指定します。

管理対象システムは、プロセッサに障害が起きた場合、区画可用性の優先順位を使用します。プロセッサが論理区画上で障害を起こし、割り当てられていない使用可能なプロセッサがその管理対象システム上にない場合、論理区画は、区画可用性の優先順位が低い方の論理区画から置換用プロセッサを獲得できます。このタスクによって、区画可用性の優先順位が高い方の論理区画は、プロセッサに障害が起きた後、実行を継続できます。

区画の区画可用性の優先順位は、区画を選択して、リストされる可用性優先順位から順位を選択することによって変更できます。

区画の優先順位付けについて詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

ワークロード・マネージメント・グループの表示

この管理対象システムに指定したワークロード管理グループの詳細を表示します。

各グループには、プロセッサの合計数、共用モード処理を使用する区画の処理単位の合計数、グループ内の区画に割り当てられたメモリーの合計量が表示されています。

システム・プロファイルの管理

システム・プロファイルは、パーティション・プロファイルを順序に従ってリストしたもので、ハードウェア管理コンソール (HMC) が使用して、管理対象システム上で特定の構成の論理区画を開始します。

システム・プロファイルを活動化すると、管理対象システムは、システム・プロファイル内の各パーティション・プロファイルを指定の順序で活動化しようとします。システム・プロファイルは、管理対象システムを活動化したり、管理対象システムを論理区画構成の1つの完全なセットから別のセットに変更したりする上で役立ちます。

リソースがオーバーコミットされているパーティション・プロファイルを含む、システム・プロファイルを作成できます。HMC を使用して、現在使用可能なリソースおよびシステム・リソースの合計に対して、システム・プロファイルを検証できます。システム・プロファイルを検証することによって、入出力装置および処理リソースがオーバーコミットされていないことを確認でき、システム・プロファイルを活動化できる可能性が高くなります。検証プロセスでは、システム・プロファイルに含まれるすべてのパーティション・プロファイルの活動化に必要なメモリー量が推定されます。システム・プロファイルが妥当性検査に合格しても、活動化するのに十分なメモリーがない場合があります。

このタスクを使用して、以下の作業を実行します。

- 新しいシステム・プロファイルを作成します。
- システム・プロファイルのコピーを作成します。
- システム・プロファイルに指定されているリソースを、管理対象システム上で使用できるリソースと比較して検証します。検証プロセスによって、システム・プロファイル内のいずれかの論理区画がすでにアクティブかどうか、また管理対象システム上のコミットされていないリソースが、パーティション・プロファイルに指定されている最小のリソースを満たすことができるかどうかを示されます。
- システム・プロファイルのプロパティを表示します。このタスクによって、既存のシステム・プロファイルを表示または変更できます。
- システム・プロファイルを削除します。
- システム・プロファイルを活動化します。システム・プロファイルを活動化すると、管理対象システムはパーティション・プロファイルをシステム・プロファイルにリストされている順序で活動化しようとします。

システム・プロファイルの管理について詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

区画データの管理

パーティション・プロファイルとは HMC のレコードであり、論理区画の可能な構成を指定します。パーティション・プロファイルを活動化すると、管理対象システムはパーティション・プロファイルの構成情報を使用して、論理区画を開始しようとします。

パーティション・プロファイルは、論理区画に必要なシステム・リソース、および論理区画が使用できるシステム・リソースの最小量と最大量を示します。パーティション・プロファイル内で指定されるシステム・リソースには、プロセッサ、メモリー、および入出力リソースなどがあります。パーティション・プロファイルでは、論理区画に特定の操作設定を指定することもできます。例えば、区画プロファイルが活動化された場合に、管理対象システムを次に電源オンした際に論理区画が自動的に開始されるように区画プロファイルを設定できます。

HMC が管理する管理対象システム上の論理区画には、それぞれ少なくとも 1 つのパーティション・プロファイルがあります。論理区画に対して、リソースの仕様が異なるパーティション・プロファイルを追加して作成できます。複数のパーティション・プロファイルを作成すると、論理区画について、いずれかのパーティション・プロファイルをデフォルトのパーティション・プロファイルに指定できます。HMC は、特定のパーティション・プロファイルを活動化するように選択しなければ、デフォルト・プロファイルを活動化します。同時にアクティブになるパーティション・プロファイルは、1 つだけです。論理区画に対して別のパーティション・プロファイルを活動化するには、論理区画をシャットダウンしてから、他のパーティション・プロファイルを活動化する必要があります。

パーティション・プロファイルは、区画 ID とプロファイル名によって識別されます。区画 ID は整数で、管理対象システム上に作成する各論理区画を識別するために使用され、プロファイル名は、各論理区画に作成するパーティション・プロファイルを識別します。論理区画上のパーティション・プロファイルの名前は、それぞれ固有のものでなければなりません。1 つの管理対象システム上の異なる論理区画では、それぞれが 1 つのプロファイル名を使用できます。例えば、論理区画 1 は **normal** という名前の複数のパーティション・プロファイルは持てませんが、**normal** という名前のプロファイルを、管理対象システム上のそれぞれの論理区画に対して作成することはできません。

パーティション・プロファイルを作成すると、HMC はシステムで使用可能なリソースをすべて表示します。HMC は、別のパーティション・プロファイルがこれらのリソースの部分を使用中かどうかは調べません。したがって、リソースをオーバーコミットする可能性があります。プロファイルを活動化すると、システムはプロファイルに割り当てられたリソースを割り当てようとします。リソースをオーバーコミットした場合、パーティション・プロファイルは活動化されません。

例えば、管理対象システムに 4 つのプロセッサがあるとします。区画 1 プロファイル A では 3 つのプロセッサ、区画 2 プロファイル B では 2 つのプロセッサが指定されています。これら 2 つのパーティション・プロファイルを同時に活動化しようとすると、プロセッサ・リソースがオーバーコミットされているため、区画 2 プロファイル B は活動化に失敗します。

論理区画をシャットダウンし、パーティション・プロファイルを使用して論理区画を再活動化する場合、パーティション・プロファイルは論理区画のリソース仕様をパーティション・プロファイルのリソース仕様でオーバーレイします。動的ロジカル・パーティショニングを使用して論理区画のリソースに加えた変

更は、パーティション・プロファイルを使用して論理区画を再度活動化したとき失われます。このアクションは、論理区画に加えた動的論理区画化の変更を元に戻す場合に必要です。ただし、管理対象システムをシャットダウンしたときに論理区画が持っていたリソース仕様を使用して論理区画を再活動化する場合は、このアクションは必要ありません。したがって、パーティション・プロファイルは最新のリソース仕様によって、最新の状態を保持するようにしてください。論理区画の現在の構成は、パーティション・プロファイルとして保管できます。このタスクにより、パーティション・プロファイルを手動で変更する必要がなくなります。

パーティション・プロファイルが最新ではない論理区画をシャットダウンする場合、かつ、管理対象システムの開始時に論理区画を自動的に開始するように設定している場合、区画の自動始動電源オン・モードを使用して管理対象システム全体を再始動することにより、その論理区画上のリソース仕様を保存することができます。論理区画は、自動的に始動した場合、管理対象システムをシャットダウンしたときにその論理区画が持っていたリソース仕様を持っています。

区画データの管理タスクを使用して、以下の作業を実行します。

- 区画データを復元する。パーティション・プロファイル・データを失った場合は、リストア・タスクを次のいずれかの方法で使用してください。
 - バックアップ・ファイルから区画データをリストアします。選択したバックアップ・ファイルが作成された後で完了したプロファイルの変更は失われます。
 - バックアップ・ファイルおよび最新のプロファイル・アクティビティからマージされたデータをリストアします。バックアップ・ファイルと最新のプロファイル・アクティビティの情報に矛盾がある場合は、バックアップ・ファイルのデータが優先されます。
 - 最新のプロファイル・アクティビティとバックアップ・ファイルからマージされたデータをリストアします。最新のプロファイル・アクティビティとバックアップ・ファイルの情報に矛盾がある場合は、最新のプロファイル・アクティビティのデータが優先されます。
- 区画データを初期化します。管理対象システムの区画データを初期化すると、現在定義されているシステム・プロファイル、区画、およびパーティション・プロファイルのすべてが削除されます。
- パーティション・プロファイルをファイルにバックアップします。
- 区画データをファイルにバックアップします。

区画データの管理について詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

使用状況データ

ハードウェア管理コンソール (HMC) が管理する特定の管理対象システムまたはすべてのシステムについて、リソース使用状況データを収集するように HMC を設定できます。

HMC は、メモリーおよびプロセッサのリソースの使用状況データを収集します。このデータを使用して、トレンドを分析し、リソースの調整を行うことができます。データは、イベントというレコードに収集されます。イベントは、次の時に生成されます。

- 定期的な間隔で (30 秒、1 分、5 分、30 分、毎時間、毎日、および毎月)。
- リソース使用率に影響を及ぼす、システム・レベルおよび区画レベルの状態変更および構成変更を行ったとき。
- HMC 上で始動、シャットダウン、およびその地方時を変更したとき。

管理対象システムについて使用状況データを収集するように HMC を設定しておかないと、管理対象システムの使用状況データを表示することはできません。

抽出率の使用可能化、設定、および変更を行ったり、抽出の収集を使用不可にしたりするには、「**抽出率の変更 (Change Sampling Rate)**」タスクを使用します。

区画の作成

最小のリソースで素早く区画を作成できます。

区画を作成するには、以下のステップを完了します。



1. ナビゲーション領域で、リソース・アイコン  をクリックしてから、「すべてのシステム」を選択します。
2. 区画を作成するサーバーを選択し、「アクション」 > 「システム区画の表示」をクリックします。
3. 「区画の作成」をクリックします。
4. 「基本区画構成 (Basic Partition Configuration)」、「プロセッサ構成」、および「メモリー構成」の各タブに必要な情報を入力します。すべてのシステム・リソースを区画に割り当てる場合は、「すべてのシステム・リソースの割り当て」チェック・ボックスを選択します。
5. 複数の区画を作成するには、スライダーに右に動かして、「複数区画の表示 (Multiple Partitions View)」を選択します。
6. 新規の区画定義を追加するには、区画表の上部にある (+) 記号をクリックします。
7. 追加された区画を選択し、「基本区画構成 (Basic Partition Configuration)」、「プロセッサ構成」、および「メモリー構成」の各タブに必要な情報を入力します。「基本区画構成」タブで、作成する区画インスタンスの数に関する詳細を指定できます。最大 20 個の区画インスタンスを作成できます。
8. 既存の区画を削除するには、削除する区画を選択して、(-) 記号をクリックします。
9. 「了解」をクリックします。

このタスクについて詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

注: 管理対象システムが仮想シリアル番号をサポートしており、管理対象システムがエンタープライズ・プール 2.0 に含まれていない場合は、「仮想シリアル番号 (Virtual Serial Number)」を「基本区画構成」タブで指定できます。

ファームウェア・レベルが FW950 で、仮想シリアル番号が割り当てられた論理区画が管理対象システムにある場合、その管理対象システムをエンタープライズ・プール 2.0 に追加することはできません。また、管理対象システムがエンタープライズ・プール 2.0 に含まれている場合は、論理区画に仮想シリアル番号を割り当てることはできません。

属性

選択した管理対象システムの属性が表示されます。この情報は、システムや区画を計画したりリソースを割り振ったりするときに役立ちます。

ご使用のシステムに使用可能な属性タスクを開くには、以下の手順を実行します。



1. ナビゲーション領域で、リソース・アイコン  をクリックしてから、「すべてのシステム」を選択します。
2. 保守容易性タスクを管理するサーバーを選択し、「アクション」 > 「システム区画の表示」をクリックします。
3. メニュー・ポッドで、「属性」を展開し、次に、実行する属性タスクをリストから選択します。

一般設定

管理対象システムの一般設定と詳細設定を表示または変更します。

これらのプロパティには、以下のタブが含まれます。

一般属性

「一般属性」タブでは、システムの名前、シリアル番号、モデルとタイプ、状態、アテンション LED の状態、サービス・プロセッサのバージョン、区画の最大数、割り当て済みサービス区画 (指定されている場合)、および電源オフ・ポリシー情報が表示されます。

移行

管理対象システムの区画モビリティ属性を表示したり管理対象システムの非アクティブ区画の移行ポリシーを変更したりします。

電源オン・パラメーター

「電源オン・パラメーター」タブから、「次の値」フィールドの値を変更することによって、次の再始動のための電源オン・パラメーターを変更できます。この変更は、管理対象システムの次の再始動についてのみに有効になります。

拡張

「拡張」タブでは、管理対象システム上のヒュージ・ページ・メモリー機能が表示され、使用可能なヒュージ・ページ・メモリー、構成可能なヒュージ・ページ・メモリー、現在のページ・サイズ、および現在の最大ヒュージ・ページ・メモリーが表示されます。ヒュージ・ページ・テーブル・サポートを備えたシステムのメモリー割り当てを変更するには、「要求されたヒュージ・ページ・メモリー (ページ)」フィールドを希望のメモリー値に設定します。ヒュージ・ページ・メモリーの要求値を変更するには、システムの電源をオフにする必要があります。

バリア同期レジスター (BSR) オプションにアレイ 情報が表示されます。

「**プロセッサ性能**」オプションには、TurboCore モードおよびシステム 区画プロセッサ制限 (SPPL) が表示されます。次の TurboCore モードと 次の SPPL 値を設定できます。SPPL は、専用プロセッサ区画と共用プロセッサ区画の両方に適用されます。

「**メモリー・ミラーリング**」オプションには、現行ミラーリング・モードおよび現行システム・ファームウェア・ミラーリング状況が表示されます。次のミラーリング・モードを設定できます。メモリー最適化ツールを開始することもできます。

VTPM 設定を表示できます。

プロセッサ、メモリー、I/O

管理対象システムのメモリー、プロセッサ、および物理 I/O リソースの設定を表示または変更します。

これらのプロパティには、以下のタブが含まれます。

プロセッサ

「**プロセッサ**」タブには、管理対象システムのプロセッサに関する情報が表示されます。この情報には、以下が含まれます。

- 取り付け済みの処理装置
- 未構成の処理装置
- 使用可能な処理装置
- 使用可能な処理装置 (スチール可能な処理装置を含む)
- 構成可能な処理装置
- 仮想プロセッサ当たりの処理装置の最小数
- 共有プロセッサ・プールの最大数

「**使用可能 (スチール可能を含む) (Available with stealable)**」フィールドには、使用可能な処理装置に関する情報が表示されます。使用可能な処理装置は、管理対象システム内の使用可能な処理装置と、スチール可能な処理装置の数の合計です。

スチール可能な処理装置の値は、管理対象システム上で電源オフまたはハイバネートされているすべての区画に割り当てられたプロセッサ・リソースの合計です。

注:

- スチール可能な処理装置に関する情報は、管理対象システムがスタンバイ 状態または稼働中状態である場合にのみ表示されます。
- 管理対象システムが Power® IFL プロセッサのライセンス交付を受けており、ファームウェア・レベルが FW910 以降である場合、「**使用可能 (スチール可能を含む) (Available with stealable)**」フィールドが表示されます。
- POWER9 システムがいくつかの IFL プロセッサのライセンス交付を受けている場合、このタブには AIX または IBM i 区画を稼働するために使用可能な残りのプロセッサに関する情報も表示されます。

メモリー

「メモリー」タブには、管理対象システムのメモリーに関する情報が表示されます。この情報には、以下が含まれます。

- インストール済みメモリー
- 未構成メモリー
- 使用可能メモリー
- 使用可能なメモリー (スチール可能なメモリーを含む)
- 構成可能なメモリー
- メモリー領域サイズ
- 区画用に使用可能な現在のメモリー
- システム・ファームウェアの現行メモリー

「使用可能 (スチール可能を含む) (Available with stealable)」フィールドには、使用可能なメモリーに関する情報が表示されます。使用可能なメモリーは、管理対象システム内の使用可能なメモリーと、スチール可能なメモリー・リソースの量の合計です。このタブには、使用可能なメモリー・プールの最大数も表示されます。

注: スチール可能なメモリーに関する情報は、管理対象システムがスタンバイ 状態または稼働中状態である場合にのみ表示されます。

物理 I/O アダプター

「物理 I/O アダプター」タブには、管理対象システムの物理 I/O リソースが表示されます。I/O スロットと区画の割り当て、アダプター・タイプ、およびスロット LP 制限情報が表示されます。物理 I/O リソース情報が装置別にグループ化されます。

- 「アダプターの説明」列には、各リソースの物理的な説明が表示されます。
- 「物理ロケーション・コード」列には、各リソースの物理ロケーション・コードが表示されます。
- 「所有者 (Owner)」列に、物理 I/O の現在の所有者が表示されます。この列の値は、以下の値のいずれであってもかまいません。
 - シングル・ルート I/O 仮想化 (SR-IOV) アダプターが共用モードの場合、この列に「ハイパーバイザー (Hypervisor)」が表示されます。
 - SR-IOV アダプターが専用モードの場合、アダプターが専用物理 I/O としていずれの区画にも割り当てられていないと、「未割り当て (Unassigned)」が表示されます。
 - SR-IOV アダプターが専用モードの場合、アダプターが専用物理 I/O としていずれかの論理区画に割り当てられていると、その論理区画名が表示されます。
- 「バス番号」列には、リソースのバス番号が表示されます。
- 「I/O プール」ボタンは、システム内で検出されたすべての I/O プール、およびそれらのプールに参加している区画を表示します。

PowerVM

ハードウェア管理コンソール (HMC) で PowerVM 機能を使用して、IBM Power Systems サーバーのシステム・レベルの仮想化機能を管理することができます。

PowerVM タスクを使用して、バーチャル I/O サーバー (VIOS)、仮想ネットワーク、仮想ストレージの構成など、システムに関連した仮想リソースを管理できます。ワークロードの変化またはパフォーマンスの強化に対応して、管理対象システム・レベルで「PowerVM の管理」機能を管理できます。

PowerVM 機能には、以下のタスクが含まれます。

- バーチャル I/O サーバーの管理
- 仮想ネットワークの管理
- 仮想ストレージの管理
- ハードウェア仮想化 I/O (SR-IOV アダプター、ホスト・イーサネット・アダプター (HEA)、およびホスト・チャンネル・アダプター (HCA)) の管理

- 予約プロセッサ・プールの管理
- 共有プロセッサ・プールの管理
- 共用メモリー・プールの管理

PowerVM の管理について詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

Capacity on Demand

管理対象サーバーに取り付けられている使用不可になっているプロセッサまたはメモリーを活動化します。

Capacity on Demand (CoD) を使用すると、プロセッサおよびメモリーを停止することなく活動化できます (ブートは必要ありません)。Capacity on Demand によって、キャパシティーを一時的に活動化して、偶発的なパフォーマンスのニーズに対応したり、必要なときに試行的に追加のキャパシティーを活動化し、また操作をサポートするキャパシティーにアクセスすることも可能です。

Capacity on Demand 機能

ご使用のシステムで利用できる各種の Capacity on Demand 機能について説明します。

Capacity on Demand (CoD) を使用すると、プロセッサおよびメモリーを停止することなく活動化できます (ブートは必要ありません)。Capacity on Demand によって、キャパシティーを一時的に活動化して、偶発的なパフォーマンスのニーズに対応したり、必要なときに試行的に追加のキャパシティーを活動化し、また操作をサポートするキャパシティーにアクセスすることも可能です。

「**Capacity on Demand プロセッサ**」機能には、以下のタスクが含まれます。

- プロセッサ設定の表示
- CUoD (永続) プロセッサ
 - CUoD コード情報の表示
- On/Off プロセッサ
 - 管理
 - 請求情報の表示
 - キャパシティー設定の表示
 - コード情報の表示
- Utility プロセッサ
 - 管理
 - キャパシティー設定の表示
 - コード情報の表示
 - 共用プロセッサ使用状況の表示
- Trial プロセッサ
 - Trial 停止
 - View capacity settings
 - コード情報の表示

「**Capacity on Demand メモリー**」機能には、以下のタスクが含まれます。

- メモリー設定の表示
- CUoD (永続) メモリー
 - CUoD コード情報の表示
- On/Off メモリー
 - 管理
 - 請求情報の表示

- キャパシティー設定の表示
- コード情報の表示
- Trial メモリー
 - Trial 停止
 - キャパシティー設定の表示
 - コード情報の表示

Capacity On Demand 機能について詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

ライセンス交付を受けた機能

管理対象システムでサポートされているランタイム 機能の表示および編集を行います。

管理対象システムでアクティブなライセンス 交付を受けた機能を確認できます。ライセンス 交付を受けた新しい機能を活動化するには、「活動化コードの入力」をクリックして、活動化コードを入力します。

管理対象システムで使用可能なライセンス 交付を受けた機能には、以下の機能があります。

- Active Memory Sharing 対応
- Live Partition Mobility 対応
- マイクロ区画化対応
- PowerVM 区画簡易リモート再始動対応
- SR-IOV 対応 (論理ポート制限)
- Virtual I/O Server 対応
- Active Memory Expansion 対応
- Active Memory Mirroring for Hypervisor 対応
- Coherent Accelerator Processor Interface (CAPI)
- AIX Enablement for 256-Core 区画対応
- 動的プラットフォーム最適化対応
- IBM i 5250 アプリケーション対応

ライセンス 交付を受けた機能について詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

保守容易性

HMC の問題分析によって、エラー条件が自動的に検出され、修復サービスが必要な問題が報告されます。

これらの問題は、サービス可能イベントとして報告されます。「サービス可能イベント・マネージャー」タスクを使用して、選択したシステムの特定のイベントを表示します。ただし、問題が起きたことに気付いたり、問題がシステムに影響を与えている疑いがあるのに、問題分析が報告してこない場合は、「サービス可能イベントの作成」タスクを使用して問題をサービス・プロバイダーに報告してください。

ご使用のシステムに使用可能な保守容易性タスクを開くには、以下の手順を実行します。



1. ナビゲーション領域で、リソース・アイコン  をクリックしてから、「すべてのシステム」を選択します。
2. 保守容易性タスクを管理するサーバーを選択し、「アクション」 > 「システム区画の表示」をクリックします。
3. メニュー・ポッドで、「保守容易性」を展開してから、「保守容易性」をクリックします。
4. 実行する保守容易性タスクをリストから選択します。

タスク・ログ

ハードウェア管理コンソール (HMC) 上で現在実行中、または完了したすべてのタスクを表示します。

タスク・ログを表示するには、以下のステップを実行します。



1. ナビゲーション領域で、「保守容易性」アイコンをクリックしてから、「タスク・ログ」を選択します。
2. タスク・ログに以下のタブが表示されます。
 - ・ **タスク名**: タスクの名前を表示します。
 - ・ **状況**: タスクの現在の状況 (実行中または完了) を表示します。
 - ・ **リソース**: リソースの名前を表示します。
 - ・ **リソース・タイプ**: リソースのタイプを表示します。
 - ・ **イニシエーター**: タスクを開始したユーザーの名前を表示します。
 - ・ **開始時刻**: タスクが開始された時刻を表示します。
 - ・ **所要時間**: タスクが完了するのに要した時間の長さを表示します。

タスク・ログの表示について詳しくは、オンライン・ヘルプを使用してください。

保守容易性

ハードウェア管理コンソール (HMC) の問題分析によって、エラー条件が自動的に検出され、修復サービスが必要な問題が報告されます。

これらの問題は、サービス可能イベントとして報告されます。「サービス可能イベント・マネージャー」タスクを使用して、選択したシステムの特定のイベントを表示します。ただし、問題が起きたことに気付いたり、問題がシステムに影響を与えている疑いがあるのに、問題分析が報告してこない場合は、「サービス可能イベントの作成」タスクを使用して問題をサービス・プロバイダーに報告してください。

ご使用のシステムに使用可能な保守容易性タスクを開くには、以下の手順を実行します。



1. ナビゲーション領域で、リソース・アイコンをクリックしてから、「すべてのシステム」を選択します。
2. 保守容易性タスクを管理するサーバーを選択し、「アクション」 > 「システム区画の表示」をクリックします。
3. メニュー・ポッドで、「保守容易性」を展開してから、「保守容易性」をクリックします。
4. 実行する保守容易性タスクをリストから選択します。

サービス可能イベント・マネージャー

管理対象システム上の問題は、ハードウェア管理コンソール (HMC) にサービス可能イベントとして報告されます。問題の表示、問題データの管理、サービス・プロバイダーへのイベントのコール・ホーム、または問題の修理が可能です。

表示するサービス可能イベントの基準を設定するには、以下の手順を実行します。



1. ナビゲーション領域で、リソース・アイコンをクリックしてから、「すべてのシステム」を選択します。
2. サービス可能イベントを管理したいサーバーを選択します。
3. メニュー・ポッドで、「保守容易性」を展開してから、「保守容易性」をクリックします。
4. 「サービス可能イベント・マネージャー」をクリックします。

5. イベント基準、エラー基準、および FRU 基準を指定します。結果をフィルターに掛けたくない場合は、「すべて」を選択します。基準フィルター値に基づいてサービス可能イベントのリストを最新表示するには、「最新表示」をクリックします。

「サービス可能イベントの概要」ウィンドウは、基準と一致するすべてのイベントを表示します。短縮テーブル・ビューに表示される情報には、以下の情報が含まれています。

- 問題番号
- PMH 番号
- 参照コード - 「参照コード」をクリックして、報告された問題の説明、および問題を修正するために実行できるアクションを表示します。
- 問題の状況
- 問題の最終報告時間
- 問題によって障害の起きた MTMS
- 発信元 HMC

表のすべてを表示すると、報告区画 ID、基本データ・イベント・タイム・スタンプ、重複カウント、通知タイプ、最初の報告時刻、報告名、報告された MTMS、ファームウェア・フィックス、およびサービス可能イベントのテキストなど、より詳細な情報が含まれます。

サービス可能イベントを選択して、「アクション」メニューを使用し、以下を行います。

- 「詳細の表示」：このイベントに関連する現場交換可能ユニット (FRU) とその説明を表示します。
- 「ファイルの表示」：選択されたサービス可能イベントに関連したファイルを表示します。
- 「参照コードの説明の表示 (View Reference Code Description)」：選択されたサービス可能イベントに関連した参照コードの説明を表示します。追加の説明がない場合、このオプションは使用できません。
- 「コール・ホーム」：イベントをサービス・プロバイダーに報告します。
- 「修復」：使用可能ならガイド付き修理手順を開始します。
- 「イベントのクローズ」：問題の解決後、コメントを追加してイベントを閉じます。
- 「PMH コメントの追加」：選択されたサービス可能イベントについて、PMH にコメントを追加します。指定された問題に PMH 番号が存在しない場合、「PMH コメントの追加」オプションは使用できません。

サービス可能イベントの管理について詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

サービス可能イベントの作成

このタスクは、ハードウェア管理コンソール (HMC) 上で発生した問題 (例えばマウスが動作しない) をサービス・プロバイダーに報告するか、問題の報告についてのテストを行います。

問題のサブミットは、このハードウェア管理コンソールがリモート・サポート機能 (RSF) を使用するようカスタマイズされ、サービスを自動的に呼び出すことが許可されているかどうかによって変わります。上記の場合、問題情報とサービス要求はモデム送信によりサービス・プロバイダーに自動的に送信されます。

ご使用のハードウェア管理コンソールに関する問題を報告する場合は、以下の手順を実行します。



1. ナビゲーション領域で、保守容易性アイコン  をクリックしてから、「サービス管理」を選択します。
2. コンテンツ・ペインで、「サービス可能イベントの作成」をクリックします。
3. 「サービス可能イベントの作成」ウィンドウに表示されるリストから問題のタイプを選択します。
4. 「問題記述」入力フィールドに問題の簡単な説明を入力して「サービスの要求」をクリックします。

「問題の報告」ウィンドウで問題の報告をテストする場合:

1. 「自動問題レポート機能のテスト」を選択して、「問題記述」入力フィールドに「単なるテストです (This is just a test)」と入力します。
2. 「サービスの要求」をクリックします。問題はハードウェア管理コンソールのサービス・プロバイダーに報告されます。問題を報告すると、「問題の報告」ウィンドウに入力した情報と、コンソールを識別するマシン情報がサービス・プロバイダーに送信されます。

問題の報告または問題の報告の動作テストについて詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

ダンプの管理

ハードウェア管理コンソール (HMC) が管理するシステムについて、システム、サービス・プロセッサ、および電源サブシステムのダンプを管理します。

システム・ダンプ

システム障害後または手動による要求後に、サーバーのハードウェアとファームウェアから収集されたデータの集まり。システム・ダンプは、次のレベルのサポートまたはサービス・プロバイダーの指示のもとでのみ実行してください。

サービス・プロセッサ・ダンプ

障害、外部のリセット、または手動による要求の後に、サービス・プロセッサから収集されたデータの集まり。

電源サブシステム・ダンプ

「大容量電源制御」サービス・プロセッサからデータが収集されます。このプロセスは、管理対象システムの特定のモデルにのみ適用されます。

「ダンプの管理」タスクを使用して、以下のタスクを完了します。

- システム・ダンプ、サービス・プロセッサ・ダンプ、または電源サブシステム・ダンプを開始します。
- ダンプを開始するにダンプ・タイプのダンプ機能パラメーターを変更します。
- ダンプを削除します。
- ダンプをメディアにコピーします。
- ファイル転送プロトコル (FTP) を使用して、別のシステムにダンプをコピーします。
- コール・ホーム機能を使用してダンプをコール・ホームして、IBM リモート・サポートなどのサービス・プロバイダーに返送し、詳細に分析してもらいます。
- ダンプの進捗にあわせてダンプのオフロード状況を表示します。

ダンプの管理について詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

VPD の収集

「重要プロダクト・データ (VPD)」を取り外し可能メディアにコピーします。

管理対象システムは、内部的に保管される VPD を持っています。VPD は、インストールされるメモリーの量や、設置されるプロセッサの数などの情報から構成されます。これらのレコードは、リモート・サービスおよびサービス担当員が、お客様が管理対象システム上のファームウェアおよびソフトウェアを最新の状態に保つのを手助けするのに使用できる重要な情報を提供できます。

注：VPD を収集するには、作動可能区画を少なくとも 1 つは保持している必要があります。詳しくは、[ロジカル・パーティショニング](#)を参照してください。

VPD ファイル内の情報は、管理対象システムについて次のようなタイプの注文を出す際に使用できます。

- 販売対象フィーチャーのインストールまたは取り外し。
- モデルをアップグレードまたはロールバックします。
- フィーチャーをアップグレードまたはロールバックします。

このタスクを使用すると、この情報を、ユーザーまたはサービス・プロバイダーが使用できるように取り外し可能メディア (ディスクセットまたはメモリー・キー) に送ることができます。

VPD の収集について詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

タイプ、モデル、フィーチャー

モデル、タイプ、マシン・タイプ・モデル・シリアル (MTMS)、またはエンクロージャーの構成 ID を編集または表示します。

拡張装置の MTMS の値または構成 ID は、置換手続き時に編集が必要な場合があります。

MTMS の編集について詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

ハードウェア操作

管理対象システムについてハードウェアを追加、交換、または除去します。インストール済みの FRU またはエンクロージャー、およびそれらのロケーションのリストを表示できます。FRU またはエンクロージャーを選択して、その装置を追加、交換、または除去するステップバイステップの手順を開始します。

ご使用のシステムに使用可能なハードウェア・タスクを開くには、以下の手順を実行します。



1. ナビゲーション領域で、リソース・アイコン  をクリックしてから、「すべてのシステム」を選択します。
2. ハードウェア・タスクを管理したいサーバーを選択します。
3. メニュー・ポッドで、「保守容易性」を展開してから、「保守容易性」をクリックします。
4. 実行するハードウェア操作タスクをリストから選択します。

ホット修復/アップグレードの準備

サービス・プロシージャの一環として、特定のハードウェア・コンポーネントを分離するために必要なアクションの要約を提供します。

許可されたサービス担当員の指示に従って、「コンポーネント・リスト」表から、修復対象のシステムのロケーション・コードを使用して、修復するコンポーネントを選択することができます。

ユニットの電源オン/オフ

「ユニットの電源オン/オフ」タスクを使用して、I/O ユニットの電源をオン/オフします。

電源をオン/オフできるのは、電源ドメイン内にあるユニットまたはスロットのみです。対応する電源オン/オフ・ボタンは、HMC から制御できないロケーション・コードに対しては使用不可になります。

FRU の追加

現場交換可能ユニット (FRU) の位置を指定して追加します。

POWER9 システムに FRU を追加するには、以下の手順を実行します。

1. 「エンクロージャー」メニューから、エンクロージャーのタイプを選択します。
2. 表示されたこのエンクロージャー用の FRU タイプのリストから FRU タイプを選択し、「次へ」をクリックします。
3. FRU ロケーションを選択してから「次へ」をクリックし、選択したロケーションに対して「FRU の追加」プロシージャを開始します。
4. ウィンドウにリストされる「プロシージャ」の詳細に従ってください。「操作」リストに、実行するプロシージャの正しい操作が表示されます。それらのプロシージャは、各操作をいつ実行するかを指示します。「操作」リストで操作を選択する前に、その操作を実行するよう助言されるまで待ってください。「次へ」をクリックして、次のサービス・プロシージャに進みます。

注：ヘッダーで FRU ロケーションのイメージを選択し、サービス対象の部品のロケーションを表示します。FRU ロケーションのイメージを別のウィンドウに拡大して表示するには、「FRU ロケーションの表示」をクリックします。

5. 最後のサービス・プロシージャを完了したら、「完了」をクリックしてサービスを終了します。

管理対象システムが POWER8® 以前の場合、FRU を追加するには、以下の手順を実行します。

1. 「FRU の追加」メニューで、エンクロージャー・タイプを選択します。
2. メニューから FRU のタイプを選択します。

3. 「次へ」をクリックします。
4. 表示されるメニューからロケーション・コードを選択します。
5. 「追加」をクリックする。
6. 「プロシーチャーの起動」をクリックします。
7. FRU のインストール・プロセスが完了したら、「完了」をクリックします。

FRU の交換

「FRU の交換」タスクを使用して、障害が発生した現場交換可能ユニット (FRU) を別の FRU と交換します。
管理対象システムが POWER9 以降の場合、FRU を交換するには、以下の手順を実行します。

1. 「エンクロージャー」メニューから、取り付け済みのエンクロージャーのタイプを選択します。
2. そのエンクロージャーについて表示された FRU タイプのリストから、交換する FRU のタイプを選択し、「次へ」をクリックします。
3. 取り付け済みの FRU ロケーションを選択してから「次へ」をクリックし、選択した FRU に対して「FRU の交換/置換」プロシーチャーを開始します。
4. ウィンドウにリストされる「プロシーチャー」の詳細に従ってください。「操作」リストに、実行するプロシーチャーの正しい操作が表示されます。それらのプロシーチャーは、各操作をいつ実行するかを指示します。「操作」リストで操作を選択する前に、その操作を実行するよう助言されるまで待ってください。「次へ」をクリックして、次のサービス・プロシーチャーに進みます。

注：ヘッダーで FRU ロケーションのイメージを選択し、サービス対象の部品のロケーションを表示します。FRU ロケーションのイメージを別のウィンドウに拡大して表示するには、「FRU ロケーションの表示」をクリックします。

5. 交換プロシーチャーが完了したら、「完了」をクリックします。

管理対象システムが POWER8 以前の場合、FRU を交換するには、以下の手順を実行します。

1. 「FRU の交換」メニューから、取り付け済みのエンクロージャー・タイプを選択します。
2. 表示されたこのエンクロージャー用の FRU タイプのリストから、FRU タイプを選択します。
3. 「次へ」をクリックして、その FRU タイプのロケーションのリストを表示します。
4. 特定の FRU のロケーション・コードを選択します。
5. 「追加」をクリックして、FRU のロケーションを「保留アクション」に追加します。
6. 「プロシーチャーの起動」を選択して、「保留アクション」にリストされている FRU の交換を開始します。
7. インストールを完了したら、「完了」をクリックします。

FRU の除去

「FRU の除去」タスクを使用して、管理対象システムから FRU を除去します。

管理対象システムが POWER9 以降の場合、FRU を取り外すには、以下の手順を実行します。

1. メニューからエンクロージャーを選択し、選択したエンクロージャーに現在取り付けられている FRU タイプのリストを表示します。
2. 選択されたシステムから取り外すことができる FRU タイプの表示されたリストから、FRU タイプを選択し、「次へ」をクリックします。
3. FRU ロケーションを選択してから「次へ」をクリックし、選択した FRU に対して「FRU の除去」プロシーチャーを開始します。
4. ウィンドウにリストされる「プロシーチャー」の詳細に従ってください。「操作」リストに、実行するプロシーチャーの正しい操作が表示されます。それらのプロシーチャーは、各操作をいつ実行するかを指示します。「操作」リストで操作を選択する前に、その操作を実行するよう助言されるまで待ってください。「次へ」をクリックして、次のサービス・プロシーチャーに進みます。

注：ヘッダーで FRU ロケーションのイメージを選択し、サービス対象の部品のロケーションを表示します。FRU ロケーションのイメージを別のウィンドウに拡大して表示するには、「FRU ロケーションの表示」をクリックします。

5. 取り外し手順が完了したら、「完了」をクリックします。

管理対象システムが POWER8 以前の場合、FRU を取り外すには、以下の手順を実行します。

1. メニューからエンクロージャーを選択し、選択したエンクロージャーに現在取り付けられている FRU タイプのリストを表示します。
2. 表示されたこのエンクロージャー用の FRU タイプのリストから、FRU タイプを選択します。
3. 「次へ」をクリックして、その FRU タイプのロケーションのリストを表示します。
4. 特定の FRU のロケーション・コードを選択します。
5. 「追加」をクリックして、FRU のロケーションを「保留アクション」に追加します。
6. 「プロシーチャーの起動」を選択して、「保留アクション」にリストされている FRU の除去を開始します。
7. 取り外し手順が完了したら、「完了」をクリックします。

エンクロージャーの追加

エンクロージャーを見つけて追加する方法について説明します。

エンクロージャーを追加するには、以下の手順を実行します。

1. エンクロージャー・タイプを選択し、「追加」をクリックします。
2. 「プロシーチャーの起動」をクリックします。
3. エンクロージャーのインストール・プロセスが完了したら、「完了」をクリックします。

エンクロージャーの除去

「エンクロージャーの除去」タスクを使用して、エンクロージャーを除去します。

エンクロージャーを取り外すには、以下の手順を実行します。

1. エンクロージャー・タイプを選択してから、「追加」をクリックして選択したエンクロージャー・タイプのロケーション・コードを「保留アクション」に追加します。
2. 「プロシーチャーの起動」をクリックして、選択したシステムから「保留アクション」で指定したエンクロージャーの除去を開始します。
3. エンクロージャーの除去プロセスが完了したら、「完了」をクリックします。

MES を開く

ハードウェア管理コンソール (HMC) でアクティブまたは非アクティブなすべての MES 操作について、MES オーダー番号とその状態を表示します。

「MES オーダー番号の追加」を使用して、新しいオーダー番号をリストに追加します。オーダー番号を追加するには、以下の手順を実行します。

1. 「MES オーダー番号の追加」をクリックします。
2. 新規 MES オーダー番号を入力します。
3. 「了解」をクリックします。

MES を閉じる

MES オーダー番号を閉じます。

「MES を閉じる」を使用して MES を閉じます。MES を閉じるには、以下の手順を実行します。

1. テーブルから、開いている MES のオーダー番号を選択します。
2. 「了解」をクリックします。

FSP フェイルオーバーのセットアップ

管理対象システムの 1 次サービス・プロセッサが障害を起こした場合は、2 次サービス・プロセッサをセットアップします。

FSP フェイルオーバーは、サービス・プロセッサのハードウェア障害によるお客様のシステム停止を減少させるように設計されています。冗長サービス・プロセッサが現在のシステム構成でサポートされて

いる場合、「**セットアップ**」を選択して、選択した管理対象システムの FSP フェイルオーバーをセットアップします。

FSP フェイルオーバーをセットアップするには、以下の手順を実行します。

1. 「**FSP フェイルオーバー**」の下にあるコンテンツ・ペインで、「**セットアップ**」をクリックします。
2. 「**了解**」をクリックして、選択したシステムの自動フェイルオーバーを有効にします。

FSP フェイルオーバーの開始

管理対象システムの 1 次サービス・プロセッサが障害を起こした場合は、2 次サービス・プロセッサを開始します。

FSP フェイルオーバーは、サービス・プロセッサのハードウェア障害によるお客様のシステム停止を減少させるように設計されています。「**開始**」を選択して、選択した管理対象システムの FSP フェイルオーバーを開始します。

FSP フェイルオーバーを開始するには、以下の手順を実行します。

1. 「**FSP フェイルオーバー**」の下にあるコンテンツ・ペインで、「**開始**」をクリックします。
2. 「**了解**」をクリックして、選択したシステムの自動フェイルオーバーを開始します。

参照コード・ログ

参照コードは、一般的な診断、トラブルシューティング、およびデバッグの情報を示します。

選択した管理対象システムについて生成された参照コードを表示します。参照コードは、診断エイドとして使用され、ハードウェアやオペレーティング・システムの問題の原因を判別するのに役立ちます。

参照コード・ヒストリーを表示するには、次の手順を完了します。



1. ナビゲーション領域で、**リソース・アイコン** をクリックしてから、「**すべてのシステム**」を選択します。
2. 保守容易性タスクを管理するサーバーを選択し、「**アクション**」 > 「**システム区画の表示**」をクリックします。
3. メニュー・ポッドで、「**保守容易性**」を展開してから、「**参照コード・ログ**」をクリックします。
4. 詳細を表示する特定の参照コードを選択します。

このタスクについて詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

RIO 構成

現在のハードウェア・トポロジおよび最新の有効ハードウェア・トポロジを表示します。

現在のハードウェア・トポロジおよび最後の有効なハードウェア・トポロジを表示します。現在のトポロジと前回の有効なトポロジとの間に矛盾があれば、エラーと見なされます。

ハードウェア・トポロジを表示するには、以下のステップを実行します。



1. ナビゲーション領域で、**リソース・アイコン** をクリックしてから、「**すべてのシステム**」を選択します。
2. 保守容易性タスクを管理するサーバーを選択し、「**アクション**」 > 「**システム区画の表示**」をクリックします。
3. メニュー・ポッドで、「**保守容易性**」を展開してから、「**RIO 構成**」をクリックします。
4. ハードウェア・トポロジ情報を表示します。

このタスクについて詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

PCI 構成

Peripheral Component Interconnect Express (PCIe) ハードウェア・トポロジに関する情報を表示します。

PCIe ハードウェア・トポロジ・ユーティリティーは、システムごとに存在する PCIe リンクに関する情報を提供します。

PCIe ハードウェア・トポロジを表示するには、以下のステップを実行します。



1. ナビゲーション領域で、リソース・アイコン  をクリックしてから、「すべてのシステム」を選択します。
2. 保守容易性タスクを管理するサーバーを選択し、「アクション」 > 「システム区画の表示」をクリックします。
3. メニュー・ポッドで、「保守容易性」を展開してから、「PCI 構成」をクリックします。
4. PCIe ハードウェア・トポロジを表示します。

このタスクについて詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

トポロジ・ダイアグラム

区画のトポロジ・ダイアグラムの表示方法を説明します。

ハードウェア管理コンソール (HMC) を使用して、区画のトポロジ・ダイアグラムを表示できます。

仮想ネットワーキング・ダイアグラムの表示

ハードウェア管理コンソール (HMC) を使用して、選択したシステムのエンドツーエンド・ネットワーク構成を表示できます。仮想ネットワークの表示は、物理アダプター・カードおよびこのカードに接続されている物理ポートで始まります。下にスクロールするにつれて、VIOS 内の定義済みの仮想ブリッジ、リンク集約デバイス、仮想スイッチ、仮想ネットワーク、および区画が表示されます。

リソースをクリックしてドラッグし、ダイアグラム全体に広げることができます。リソースをダブルクリックして、そのリソース、およびネットワーク内でのその各種仮想コンポーネントと物理コンポーネントとの関係を強調表示することもできます。強調表示を解除するには、ネットワーク・ダイアグラムの空の領域でダブルクリックしてください。リソースに関する詳細情報を表示するには、目的のリソースを右クリックすると、クリック・カードに追加情報が表示されます。別の方法として、リソース・エリアのラベルの上にカーソルを移動させると、ツールチップとしてリソースの名前を表示できます。

HMC を使用して、選択したシステムのエンドツーエンド・ネットワーク構成を表示するには、以下の手順を完了します。



1. ナビゲーション領域で、リソース・アイコン  をクリックしてから、「すべてのシステム」を選択します。
2. 保守容易性タスクを管理するサーバーを選択し、「アクション」 > 「システム区画の表示」をクリックします。
3. メニュー・ポッドで、「トポロジ」を展開してから、「仮想ネットワーキング・ダイアグラム」をクリックします。
4. 選択したシステムのリソースを右クリックして、クリック・カードにさらに詳しい情報を表示します。リソース・エリアのラベルの上にカーソルを移動させて、ツールチップとしてリソースの名前を表示することもできます。
5. 作業ペインの右上隅で、「ズームイン」および「ズームアウト」のアイコンをクリックして、表示を必要なレベルの倍率にします。

注：ダイアグラム内でマウスのスクロール・ホイールを使用して、ズームインおよびズームアウトを行うこともできます。

6. 作業ペインの右上隅で、「凡例」アイコンをクリックして、仮想ネットワーキング・ダイアグラムで使われるシンボルの説明を表示します。

このタスクについて詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

仮想ストレージ・ダイアグラムの表示

2つのタイプの仮想ストレージ・ダイアグラム、つまり、システム・ストレージと区画ストレージが用意されています。HMCを使用することで、選択したシステムの仮想ストレージ構成を、システム・ストレージの物理コンポーネントと仮想コンポーネントを含めて表示できます。ハードウェア管理コンソール (HMC) を使用することにより、特定の区画に割り当てられたストレージの物理コンポーネントおよび仮想コンポーネントを含め、特定のシステム内の単一区画の仮想ストレージ構成を表示することもできます。

このダイアグラムには、システムまたは単一区画のコンテンツの概要が示されます。特定のコンポーネントの関係は示されません。リソースをクリックしてドラッグし、ダイアグラム全体に広げることができます。リソースをダブルクリックして、そのリソース、およびネットワーク内でのその各種仮想コンポーネントと物理コンポーネントとの関係を強調表示することもできます。強調表示を解除するには、ストレージ・ダイアグラムの空の領域でダブルクリックしてください。リソースに関する詳細情報を表示するには、目的のリソースを右クリックすると、クリック・カードに追加情報が表示されます。別の方法として、リソース・エリアのラベルの上にカーソルを移動させると、ツールチップとしてリソースの名前を表示できます。

HMCを使用して、選択したシステムまたは単一区画の仮想ストレージ構成を表示するには、以下の手順を実行します。

1. ナビゲーション領域で、リソース・アイコン  をクリックしてから、「すべてのシステム」を選択します。
2. 保守容易性タスクを管理するサーバーを選択し、「アクション」 > 「システム区画の表示」をクリックします。
3. メニュー・ポッドで、「トポロジー」を展開してから、「仮想ストレージ・ダイアグラム」をクリックします。

注: 特定のシステム内の単一区画の仮想ストレージ・ダイアグラムを表示するには、任意の区画を選択してから、「トポロジー」を展開し、「区画仮想ストレージ・ダイアグラム」をクリックしてください。

4. 選択したシステムのリソースを右クリックして、クリック・カードにさらに詳しい情報を表示します。リソース・エリアのラベルの上にカーソルを移動させて、ツールチップとしてリソースの名前を表示することもできます。
5. 作業ペインの右上隅で、「ズームイン」および「ズームアウト」のアイコンをクリックして、表示を必要なレベルの倍率にします。

注: ダイアグラム内でマウスのスクロール・ホイールを使用して、ズームインおよびズームアウトを行うこともできます。

6. 作業ペインの右上隅で、「凡例」アイコンをクリックして、仮想ストレージ・ダイアグラムで使われるシンボルの説明を表示します。

このタスクについて詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

SR-IOV ダイアグラムおよび vNIC ダイアグラムの表示

ハードウェア管理コンソール (HMC) を使用することで、選択したシステムの SR-IOV および仮想ネットワーク・インターフェース・コントローラー (vNIC) 構成を、システム・ストレージの物理コンポーネントと仮想コンポーネントを含めて表示できます。

このダイアグラムには、SR-IOV アダプターとその他の仮想コンポーネント (例えば vNIC) との関係が示されます。リソースをクリックしてドラッグし、ダイアグラム全体に広げることができます。リソースをダブルクリックして、そのリソース、およびネットワーク内でのその各種仮想コンポーネントと物理コンポーネントとの関係を強調表示することもできます。強調表示を解除するには、SR-IOV および vNIC ダイアグラムの空の領域でダブルクリックしてください。リソースに関する詳細情報を表示するには、目的のリ

ソースを右クリックすると、クリック・カードに追加情報が表示されます。別の方法として、リソース・エリアのラベルの上にカーソルを移動させると、ツールチップとしてリソースの名前を表示できます。

HMC を使用して、選択したシステムのエンドツーエンド・ネットワーク構成を表示するには、以下の手順を完了します。



1. ナビゲーション領域で、リソース・アイコン  をクリックしてから、「すべてのシステム」を選択します。
2. 保守容易性タスクを管理するサーバーを選択し、「アクション」 > 「システム区画の表示」をクリックします。
3. メニュー・ポッドで、「トポロジー」を展開してから、「SR-IOV vNIC ダイアグラム」をクリックします。
4. 選択したシステムのリソースを右クリックして、クリック・カードにさらに詳しい情報を表示します。リソース・エリアのラベルの上にカーソルを移動させて、ツールチップとしてリソースの名前を表示することもできます。
5. 作業ペインの右上隅で、「ズームイン」および「ズームアウト」のアイコンをクリックして、表示に必要なレベルの倍率にします。

注：ダイアグラム内でマウスのスクロール・ホイールを使用して、ズームインおよびズームアウトを行うこともできます。

6. 作業ペインの右上隅で、「凡例」アイコンをクリックして、SR-IOV および vNIC のダイアグラムで使用されているシンボルの説明を表示します。

このタスクについて詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

システム管理 (区画)

「システム管理」は、サーバー、論理区画、およびフレームを管理するために実行可能なタスクを表示します。これらのタスクを使用して、区画のセットアップおよび構成を行い、現在の状態を表示し、トラブルシューティングを行い、さらに解決策を適用します。

以下のタスクのセットは、区画が選択されると示され、メニュー・ポッドまたはコンテンツ・ペインに表示されます。メニュー・ポッドにリストされるタスクは、作業域で選択を行うと変わります。

区画コンテンツ・ペイン

管理コンソールに接続されているすべての区画の状態、正常性、およびキャパシティー情報を表示およびモニターします。

ウィンドウの中央部分にあるコンテンツ・ペインには、すべての使用可能な区画と、各区画の関連情報が表示されます。

各区画について、現在の区画の状態、参照コード、割り振られている仮想プロセッサの数、および割り振られているランダム・アクセス・メモリー (RAM) の量が表示されます。さらに、表形式のビューを選択した場合は、表の右上隅にあるドロップダウン矢印を選択することで、表示される情報をフィルタリングすることができます。表に表示したいフィールドに対応するチェック・ボックスを選択します。HMC バージョン 9.1.930 以降を使用している場合は、「すべての区画」表で、管理対象システムに関連付けられているすべての区画のメモリー・モードを表示することもできます。

「属性」アイコンをクリックして、以下の情報を表示することができます。

- 現在の状態
- システム名
- 参照コード
- 区画 ID
- IP アドレス (IP address)
- 環境

- OS バージョン
- RMC 接続
- 前回活動化したプロファイル
- 物理 I/O を含む
- グループ・タグ
- アテンション LED

「**capacity**」アイコンをクリックして、以下の情報を表示することができます。

- 収集の日付。
- プロセッサ使用状況 (タイプ (専用、上限なし、上限あり)、許容キャパシティー、および仮想プロセッサ)。プロセッサ・タイプが「専用」の場合、棒グラフと数値によって、使用プロセッサの使用率 (「使用」を「割り当て済み」で除算) がパーセンテージで示されます。棒グラフのしきい値ラインは、ピークしきい値 (「ピーク」を「割り当て済み」で除算) を示します。プロセッサ・タイプが「上限なし」の場合、棒グラフと数値によって、使用プロセッサの使用率 (「使用」を仮想プロセッサの数で除算) がパーセンテージで示されます。棒グラフのしきい値ラインは、ピークしきい値 (「ピーク」を仮想プロセッサの数で除算) を示します。プロセッサ・タイプが「上限あり」の場合、棒グラフと数値によって、使用プロセッサの使用率 (「使用」を「資格あり」で除算) がパーセンテージで示されます。棒グラフのしきい値ラインは、ピークしきい値 (「ピーク」を「資格あり」で除算) を示します。値がしきい値を超えると、棒グラフの書式が破線に変更されます。
- メモリー割り当て (割り当て済み)。
- ネットワーク I/O 使用状況 (1 秒当たりの送信および受信テラバイト数、および 1 秒当たりのパケット数)。棒グラフと数値によって、平均使用率 ((平均転送バイト数をアダプター数で除算した値) を最大転送バイト数で除算) がパーセンテージで示されます。棒グラフのしきい値ラインは、上限しきい値 (最大転送バイト数) を示します。値がしきい値を超えると、棒グラフの書式が破線に変更されます。
- ストレージ I/O 使用状況 (1 秒当たりの書き込みおよび読み取り情報量 (キロバイト数))。棒グラフと数値によって、平均使用率 ((平均転送バイト数をアダプター数で除算した値) を最大転送バイト数で除算) がパーセンテージで示されます。棒グラフのしきい値ラインは、上限しきい値 (最大転送バイト数) を示します。値がしきい値を超えると、棒グラフの書式が破線に変更されます。
- データ収集。

区画の属性

「**区画属性の表示**」タスクは、選択した区画の属性を表示します。この情報はリソースの割り振りおよび区画の管理に役立ちます。次のプロパティーが含まれます。

一般

「**一般**」タブには、区画の名前、ID、環境、状態、リソース構成、オペレーティング・システム、オペレーティング・システムを始動するブート・モード、および区画が配置されているシステムが表示されます。

注: 管理対象システムが仮想シリアル番号をサポートしており、管理対象システムがエンタープライズ・プール 2.0 に含まれていない場合は、「仮想シリアル番号 (Virtual Serial Number)」プロパティーが「**一般**」タブに表示されます。

「**詳細設定**」をクリックすると、論理区画のサポート対象ハードウェア・アクセラレーターおよび特定のハードウェア・アクセラレーターのサービス品質 (QoS) クレジットのリストも表示されます。管理対象システムがハードウェア・アクセラレーターをサポートしていない場合、このセクションは表示されません。

注: HMC が V9.2.950.0 以降であり、ファームウェア・レベルが FW950 以降の場合は、論理区画の鍵ストア・サイズとして、「**鍵ストア・サイズ (KeyStore Size)**」値を 4 KB から 64 KB までの範囲で選択できます。0 KB という値は、その論理区画に対して鍵ストア機能が使用不可であることを示しています。

プロセッサ

「**プロセッサ**」タブでは、プロセッサの現在の使用状況が表示されます。

注：オペレーティング・システムおよびハイパーバイザーが、仮想プロセッサごとに 0.05 プロセッサの最小ライセンスをサポートする場合、最小、最大、および希望する処理装置は、0.05 の最小サポート値に設定することができます。

メモリー

「メモリー」タブでは、専用メモリーまたは共用メモリーを使用している実行中の論理区画の属性が表示されます。

物理 I/O アダプター

「物理 I/O アダプター」タブでは、管理対象システムで使用可能であり、区画に割り当て可能なすべての物理 I/O アダプターの属性が表示されます。また、区画内のアダプターを追加および除去することもできます。

デフォルト・プロファイルの変更

区画のデフォルト・プロファイルを変更します。

新しいデフォルト・プロファイルにするプロファイルをドロップダウン・リストから選択します。

操作

「操作」には、区画を操作するタスクが含まれています。

このタスクについて

ご使用の区画に使用可能な操作タスクを開くには、以下の手順を実行します。

1. ナビゲーション領域で、リソース・アイコン  をクリックしてから、「すべてのパーティション」を選択します。
2. 操作タスクを管理したい区画を選択します。「アクション」 > 「区画属性の表示」をクリックします。
3. メニュー・ポッドで、「区画アクション」を展開してから、「操作」を展開します。
4. 実行する操作タスクをリストから選択します。

活動化

「活動化」タスクを使用して、管理対象システム上で「活動化されていない」状態にある区画を活動化します。

区画のプロファイルをプロファイルのリストから選択して「了解」をクリックし、区画を活動化します。「Advanced」タブで、「No VSI Profile」チェック・ボックスを選択し、Virtual Station Interface (VSI) を構成している間の障害を無視します。

注：HMC バージョン 7.7 以降では、DVD、保存されたイメージ、または Network Installation Management (NIM) サーバーを使用して、HMC から論理区画上にバーチャル I/O サーバー (VIOS) をインストールできます。

Netboot

netboot タスクを使用して、「非活動」状態の管理対象システム上の AIX、Linux、または IBM i 区画をネットワーク・ブートします。

「ネットワーク・ブート」ウィザードでは、区画にオペレーティング・システムをインストールし、区画を活動化するための手順がガイドされます。区画にオペレーティング・システムをインストールするには、パーティション・プロファイルを選択します。論理区画のネットワーク設定を構成するには、「次へ」をクリックします。

注：Virtual I/O Server の場合、「非活動」状態の管理対象システムに VIOS をインストールするには、「アクション」メニューから「インストール」オプションを選択する必要があります。

再始動

選択した論理区画 (複数可) を再始動します。

IBM i 論理区画に対してこのウィンドウを使用できるのは、オペレーティング・システムのコマンド行から IBM i 論理区画を再始動できない場合に限定されます。このウィンドウを使用して IBM i 論理区画を再始動すると、異常な IPL が行われることになります。

多数のクライアント区画のページング・サービス区画 (PSP) として活動している VIOS 区画の再始動を選択すると、VIOS 区画をシャットダウンする前にクライアント区画のシャットダウンが必要であることを指示する警告が表示されます。

次のどちらかのオプションを選択します。「オペレーティング・システム」オプションと「オペレーティング・システムの即時」オプションは、Resource Monitoring and Control (RMC) が起動されて構成済みの場合にのみ使用可能です。

ダンプ

HMC は、論理区画をシャットダウンし、主ストレージのダンプまたはシステム・メモリーのダンプを開始します。AIX および Linux の論理区画の場合、HMC は論理区画にもシャットダウンする旨を通知します。IBM i 論理区画の場合は、プロセッサが即時に停止します。シャットダウンの完了後、論理区画は即時に再始動します。(IBM i 論理区画は複数回再始動され、論理区画がダンプ情報を保管できるようにします)。このオプションは、オペレーション・システムの一部がハングし、解析のため論理区画のダンプが必要な場合に使用してください。

オペレーティング・システム

HMC は、論理区画に対して shutdown -r コマンドを発行して、論理区画を通常のとおりシャットダウンします。この操作の間、論理区画は必要なシャットダウン・アクティビティーを実行します。シャットダウンの完了後、論理区画は即時に再始動します。このオプションは AIX 論理区画でのみ指定できます。即時: HMC は、論理区画を即時にシャットダウンします。HMC は、すべてのアクティブ・ジョブを即時に終了します。それらのジョブで実行中のプログラムは、ジョブのクリーンアップを行うことができません。データが部分的に更新されている場合には、このオプションによって不適切な結果が生じる可能性があります。このオプションは、制御された終了に失敗したときにのみ使用してください。

オペレーティング・システムの即時

HMC は、論理区画に shutdown -Fr コマンドを発行して、論理区画を即時にシャットダウンします。この操作の間、論理区画は他のユーザーへのメッセージおよび他のシャットダウン・アクティビティーを省略します。シャットダウンの完了後、論理区画は即時に再始動します。このオプションは AIX 論理区画でのみ指定できます。

ダンプ再試行

HMC は、論理区画上で主ストレージのダンプまたはシステム・メモリーのダンプを再試行します。この操作の完了後、論理区画はシャットダウンしてから再始動します。このオプションは、以前に「ダンプ」オプションを試行して失敗している場合にのみ使用してください。このオプションは IBM i 論理区画でのみ指定できます。

シャットダウン

選択した論理区画 (複数可) をシャットダウンします。

IBM i 論理区画に対してこのウィンドウを使用できるのは、オペレーティング・システムのコマンド行から IBM i 論理区画をシャットダウンできない場合に限定されます。このウィンドウを使用して IBM i 論理区画をシャットダウンすると、異常な IPL が行われることになります。

多数のクライアント区画のページング・サービス区画 (PSP) として活動している VIOS 区画のシャットダウンを選択すると、VIOS 区画をシャットダウンする前にクライアント区画をシャットダウンするよう指示する警告が表示されます。

以下のオプションから選択してください。

遅延

HMC は、論理区画を遅延電源オフ手順を使用してシャットダウンします。これによって、論理区画には、ジョブを終了し、データをディスクに書き込む時間が与えられます。論理区画が事前指定された

時間内にシャットダウンできない場合、その区画は異常終了し、次の再始動は通常より時間がかかる場合があります。

即時

HMC は、論理区画を即時にシャットダウンします。HMC は、すべてのアクティブ・ジョブを即時に終了します。それらのジョブで実行中のプログラムは、ジョブのクリーンアップを行うことができません。データが部分的に更新されている場合には、このオプションによって不適切な結果が生じる可能性があります。このオプションは、制御されたシャットダウンを試行して失敗したときにのみ使用してください。

オペレーティング・システム

HMC は、論理区画に shutdown コマンドを発行して、論理区画を通常のとおりシャットダウンします。この操作の間、論理区画は必要なシャットダウン・アクティビティーを実行します。このオプションは AIX 論理区画でのみ指定できます。

オペレーティング・システムの即時

HMC は、論理区画に shutdown -F コマンドを発行して、論理区画を即時にシャットダウンします。この操作の間、論理区画は他のユーザーへのメッセージおよび他のシャットダウン・アクティビティーを省略します。このオプションは AIX 論理区画でのみ指定できます。

削除

「削除」タスクを使用して、選択した区画を削除します。

「削除」タスクは、選択した区画およびその区画に関連するすべてのパーティション・プロファイルを、管理対象システムから削除します。区画を削除すると、その区画に現在割り当てられているすべてのハードウェア・リソースは、他の区画が使用できるようになります。

操作のスケジュール

論理区画上で実行する特定の操作のスケジュールを作成します。

システム操作の自動処理、遅延処理、または反復処理が必要な状況では、スケジュール操作が便利です。スケジュール操作は、指定した時刻に、オペレーターが操作の実行に携わることなく開始します。スケジュールには、1 回の操作または複数回の繰り返しを設定できます。

例えば、リソースを論理区画から除去する操作や、ある論理区画から別の論理区画にリソースを移動する操作をスケジュールできます。

「スケジュール操作」タスクは、各操作について次の情報を表示します。

- 操作の対象になるプロセッサ
- スケジュールされている日付
- スケジュールされている時刻
- 操作
- 残されている繰り返し回数

「スケジュール操作」ウィンドウでは、以下の操作を実行できます。

- 操作を後で実行するようスケジュールします。
- 操作を定期的な間隔で繰り返し実行するように定義します。
- スケジュール操作を削除します。
- 現在スケジュールされている操作の詳細を表示します。
- 指定した時刻範囲内にスケジュールされている操作を表示します。
- スケジュールされている操作を、日付、操作、または管理対象システム別にソートします。

ある操作が一度実行されるようにスケジュールするか、またはそれが繰り返し実行されるようにスケジュールすることができます。操作が実行される時刻および日付を指定する必要があります。操作を繰り返し実行させたい場合、以下の時間間隔を選択する必要があります。

- 操作を実行する曜日 (任意)

- 操作の実行間隔または時刻 (必須)
- 繰り返しの合計回数 (必須)

論理区画に対してスケジュールできる操作には、以下の操作が含まれます。

LPAR に対する活動化

選択した論理区画を活動化するために、選択したプロファイルに基づいて操作をスケジュールします。

動的再構成

リソース (プロセッサまたはメガバイト・クラスのメモリー) の追加、除去、または移動の操作をスケジュールします。

オペレーティング・システムをシャットダウンします (区画上で)。

選択した論理区画のシステム・シャットダウンをスケジュールします。

HMC 上の操作をスケジュールするには、以下のステップを完了します。

1. ナビゲーション領域で、「**システム管理**」をクリックします。
2. 作業ペインで、1 つ以上の区画を選択します。
3. タスクパッドで、「**操作**」タスク・カテゴリーを選択してから「**操作のスケジュール**」をクリックします。「**スケジュール操作のカスタマイズ (Customize Scheduled Operations)**」ウィンドウが開きます。
4. 「**スケジュール操作のカスタマイズ (Customize Scheduled Operations)**」ウィンドウから、メニューバーの「**オプション (Options)**」をクリックし、オプションの次のレベルを表示します。
 - スケジュール操作を追加するには、「**オプション**」をクリックしてから「**新規**」をクリックします。
 - スケジュール操作を削除するには、削除する操作を選択して「**オプション**」を選択してから「**削除**」をクリックします。
 - 選択したオブジェクトについて、スケジュール操作のリストを現在のスケジュールで更新するには、「**オプション**」を選択してから「**最新表示**」をクリックします。
 - スケジュール操作を表示するには、表示する操作を選択して「**表示**」を選択してから「**スケジュールの詳細**」をクリックします。
 - スケジュール操作の時間を変更するには、変更する操作を選択して「**表示**」を選択してから「**新しい時間範囲**」をクリックします。
 - スケジュール操作をソートするには、「**ソート**」を選択してから表示されるソート・カテゴリーのいずれかをクリックします。
5. HMC ワークスペースに戻るには、「**操作**」を選択してから「**終了**」をクリックします。

保守準備状況の検証

Virtual I/O Server (VIOS) の保守準備状況を検証するには、「**保守準備状況の検証**」タスクを使用します。VIOS に対して検証操作を行うには、VIOS がアクティブな Resource Monitoring and Control (RMC) 接続を使用して「**実行中**」状態でなければなりません。検証操作を実行するには、管理対象システムのすべての区画に対するアクセス権限を持っている必要があります。

ハードウェア管理コンソール (HMC) は、保守のための VIOS の準備状況を検証します。保守準備状況の操作を実行すると、HMC は、マルチパス I/O 操作や、論理区画に接続したネットワークとストレージの冗長性セットアップに Virtual I/O Server を使用するすべてのクライアント論理区画を検証します。ネットワークやストレージの冗長性セットアップを確認するために、HMC は管理対象システムに関連付けられている他の Virtual I/O Server のインベントリー情報を取得します。ただし、システム内の他の VIOS 区画に適正な RMC 接続がない場合は、検証プロセスが続行され、結果が Virtual I/O Server の現在の状態に基づいて表示されます。

そのページには、影響を受けるすべてのクライアント区画に関する情報も表示されます。それらのクライアント区画には、冗長な仮想 SCSI ストレージや仮想ファイバー・チャネル、仮想ネットワーク、および VIOS が提供する仮想 NIC がありません。

モビリティー

「モビリティー」タスクは、区画を別のサーバーに移行し、移行の要件が満たされていることを確認し、区画が無効な状態になっている場合はリカバリーするのに使用します。

移行

別の管理対象システムに区画を移行します。

このタスクについて

区画を別のシステムに移行するには、以下の手順を実行します。

手順



1. ナビゲーション領域で、リソース・アイコン  をクリックしてから、「すべてのシステム」を選択します。
2. コンテンツ・ペインで、該当のサーバーを選択します。「アクション」 > 「システム区画の表示」をクリックします。
3. コンテンツ・ペインで、別のシステムに移行したい区画を選択します。
4. 「アクション」 > 「モビリティー」 > 「移行」をクリックします。「区画の移行」ウィザードが開きます。
5. 「区画の移行」ウィザードのステップを完了して、「終了」をクリックします。

検証

移動元システムから宛先システムへ区画を移動するための設定を検証します。

このタスクについて

設定を検証するには、以下の手順を実行します。

手順



1. ナビゲーション領域で、リソース・アイコン  をクリックしてから、「すべてのシステム」を選択します。
2. コンテンツ・ペインで、該当のサーバーを選択します。「アクション」 > 「システム区画の表示」をクリックします。
3. コンテンツ・ペインで、設定を検証したい区画を選択します。
4. 「アクション」 > 「モビリティー」 > 「検査」をクリックします。「区画の移行の検証」ウィンドウが開きます。
5. フィールドに情報を入力して、「検証」をクリックします。

リカバリー

完了していない移行からこの区画をリカバリーします。

このタスクについて

完了していない移行からこの区画をリカバリーするには、以下の手順を実行します。

手順



1. ナビゲーション領域で、リソース・アイコン  をクリックしてから、「すべてのシステム」を選択します。

2. コンテンツ・ペインで、該当のサーバーを選択します。「アクション」 > 「システム区画の表示」をクリックします。
3. コンテンツ・ペインで、リカバリーしたい区画を選択します。
4. 「アクション」 > 「モビリティ」 > 「リカバリー」をクリックします。「移行のリカバリー」ウィンドウが開きます。
5. 必要に応じて情報を入力して、「リカバリー」をクリックします。

区画のテンプレート

区画のテンプレートには、物理アダプター、仮想ネットワーク、およびストレージ構成などの区画リソースに関する詳細が含まれています。ハードウェア管理コンソール (HMC) 上の、テンプレート・ライブラリーで入手できるクイック・スタートのテンプレートから、または独自のユーザー定義テンプレートから、クライアント区画を作成することができます。

区画をテンプレートとして取り込む

ハードウェア管理コンソール (HMC) を使用して、稼働中区画の構成詳細を取り込み、その情報を区画テンプレートとして保存することができます。

構成をテンプレートとして取り込むには、以下のステップを実行します。

1. ナビゲーション領域で、リソース・アイコン  をクリックしてから、「すべてのパーティション」を選択します。
2. テンプレートとして取り込む区画を選択します。
3. 「アクション」 > 「テンプレート」 > 「区画をテンプレートとして取り込む」をクリックします。
4. テンプレート名と説明を入力します。
5. 「了解」をクリックします。

このタスクについて詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

プロファイル

「プロファイル」メニューで使用可能なタスクについて説明します。

プロファイルの管理

「プロファイルの管理 (Manage Profiles)」タスクを使用して、選択した区画のプロファイルを作成、編集、コピー、削除、または活動化します。

パーティション・プロファイルには、その区画のリソース構成が含まれています。プロファイルのプロセッサ、メモリー、およびアダプターの割り当ては、そのプロファイルを編集することによって変更できます。

論理区画のデフォルトパーティション・プロファイルは、他のパーティション・プロファイルが選択されていない場合、その論理区画を活動化するために使用するパーティション・プロファイルです。デフォルトのパーティション・プロファイルは、最初に別のパーティション・プロファイルをデフォルトパーティション・プロファイルとして指定しない限り、削除できません。デフォルト・プロファイルは状況列で定義されます。

「コピー」を選択して、選択したパーティション・プロファイルの正確なコピーを作成します。これを使用し、パーティション・プロファイルをコピーして必要に応じて変更することによって、互いにほぼ同一のパーティション・プロファイルを複数作成できます。

カスタム・グループの管理

グループは、オブジェクトを論理的に収集して構成したものです。状況をグループ別にレポートすることによって、システムが選択した状況にあることをモニターできます。グループはネストもできる (グループ内にグループを含める) ため、階層表示またはトポロジー表示ができます。

既に1つ以上のユーザー定義グループが、ご使用のハードウェア管理コンソール (HMC) で定義されている場合があります。デフォルト・グループは、「構成」の下にある「カスタム・グループ」ノードの下にリストされます。デフォルト・グループは、「すべての区画」と「すべてのオブジェクト」です。「カスタム・グループの管理」タスクを使用して、他のグループを作成したり、作成したグループを削除、作成したグループにグループを追加、パターン・マッチング方式を使用してグループを作成、または作成したグループからグループを削除することができます。

カスタム・グループの管理について詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

現在の構成の保管

論理区画の現在の構成を、新しいパーティション・プロファイルの名前を入力することによって、そのパーティション・プロファイルに保管できます。

この手順は、動的ロジカル・パーティショニングを使用して論理区画の構成を変更し、その変更内容を論理区画を再始動したとき失わないようにする場合、役に立ちます。この手順は、論理区画を最初に活動化した後、いつでも実行できます。

区画の削除

ハードウェア管理コンソール (HMC) を使用して、区画および関連する区画プロファイルを削除することができます。

区画を削除するには、以下のステップを実行します。

1. ナビゲーション領域で、リソース・アイコン  をクリックしてから、「すべてのパーティション」を選択します。
2. 削除したい区画を選択します。
3. 「アクション」 > 「区画の削除」をクリックします。
4. 必要なオプションを選択します。
5. 「了解」をクリックします。

このタスクについて詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

保守容易性

HMC の問題分析によって、エラー条件が自動的に検出され、修復サービスが必要な問題が報告されます。

これらの問題は、サービス可能イベントとして報告されます。「サービス可能イベント・マネージャー」タスクを使用して、選択したシステムの特定のイベントを表示します。ただし、問題が起きたことに気付いたり、問題がシステムに影響を与えている疑いがあるのに、問題分析が報告してこない場合は、「サービス可能イベントの作成」タスクを使用して問題をサービス・プロバイダーに報告してください。

サービス可能イベント・マネージャー

管理対象区画に関する問題は、ハードウェア管理コンソール (HMC) にサービス可能イベントとして報告されます。問題の表示、問題データの管理、サービス・プロバイダーへのイベントのコール・ホーム、または問題の修理が可能です。

表示するサービス可能イベントの基準を設定するには、以下の手順を実行します。



1. ナビゲーション領域で、リソース・アイコン  をクリックしてから、「すべてのシステム」を選択します。
2. サービス可能イベントを管理したいサーバーを選択します。
3. メニュー・ポッドで、「保守容易性」を展開してから、「保守容易性」をクリックします。
4. 「サービス可能イベント・マネージャー」をクリックします。
5. イベント基準、エラー基準、および FRU 基準を指定します。フィルタリングされた結果を必要としない場合は、「すべて」を選択します。基準フィルター 値に基づいてサービス可能イベントのリストを最新表示するには、「最新表示」をクリックします。

「サービス可能イベントの概要」ウィンドウは、基準と一致するすべてのイベントを表示します。短縮テーブル・ビューに表示される情報には、以下の情報が含まれています。

- 問題番号
- PMH 番号
- 参照コード - 「参照コード」をクリックして、報告された問題の説明、および問題を修正するために実行できるアクションを表示します。
- 問題の状況
- 問題の最終報告時間
- 問題によって障害の起きた MTMS
- 発信元 HMC

表のすべてを表示すると、報告区画 ID、基本データ・イベント・タイム・スタンプ、重複カウント、通知タイプ、最初の報告時刻、報告名、報告された MTMS、ファームウェア・フィックス、およびサービス可能イベントのテキストなど、より詳細な情報が含まれます。

サービス可能イベントを選択して、「アクション」ドロップダウン・メニューを使用し、以下を行います。

- 「詳細の表示」：このイベントに関連する現場交換可能ユニット (FRU) とその説明を表示します。
- 「ファイルの表示」：選択されたサービス可能イベントに関連したファイルを表示します。
- 「参照コードの説明の表示 (View Reference Code Description)」：選択されたサービス可能イベントに関連した参照コードの説明を表示します。追加の説明がない場合、このオプションは使用できません。
- 「コール・ホーム」：イベントをサービス・プロバイダーに報告します。
- 「修復」：使用可能ならガイド付き修理手順を開始します。
- 「イベントのクローズ」：問題の解決後、コメントを追加してイベントを閉じます。
- 「PMH コメントの追加」：選択されたサービス可能イベントについて、PMH にコメントを追加します。指定された問題に PMH 番号が存在しない場合、「PMH コメントの追加」オプションは使用できません。

サービス可能イベントの管理について詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

参照コード・ログ

「参照コード・ログ」タスクを使用して、選択した論理区画用に生成された参照コードを表示します。参照コードは、診断エイドとして使用され、ハードウェアやオペレーティング・システムの問題の原因を判別するのに役立ちます。

デフォルトでは、論理区画が生成した最新の参照コードのみが表示されます。追加の参照コードを表示するには、表示したい参照コードの個数を「履歴の表示」に入力して、「最新表示」をクリックします。指定された個数の最新の参照コードが、それぞれの参照コードが生成された日付と時刻とともに、ウィンドウに表示されます。ウィンドウには論理区画用に保管される参照コードの最大数まで表示できます。

コントロール・パネル機能

このタスクは、選択した IBM i 区画の使用可能な仮想コントロール・パネル機能を表示します。次のタスクがあります。

(21) 専用サービス・ツールの活動化

区画上で専用サービス・ツール (DST) を開始します。

(65) リモート・サービスの使用不可化

区画上でリモート・サービスを非活動化します。

(66) リモート・サービスの使用可能化

区画上でリモート・サービスを活動化します。

(68) 並行保守電源オフ・ドメイン

並行保守電源ドメインの電源オフ。

(69) 並行保守電源オン・ドメイン

並行保守電源ドメインの電源オン。

仮想 I/O

仮想ネットワーク、仮想ネットワーク・インターフェース・コントローラー、および区画の仮想ストレージの表示方法について説明します。

ハードウェア管理コンソール (HMC) を使用して、区画の仮想トポロジを表示できます。

仮想ネットワーク

選択した論理区画に関連付けられている仮想ネットワークの表示および追加を行えます。

「仮想ネットワーク」テーブルには、各仮想ネットワークに関連付けられている仮想ネットワーク名、VLAN ID、仮想スイッチ、仮想ネットワーク・ブリッジ、および仮想イーサネット・アダプター ID がリストされます。「**仮想ネットワークの接続 (Attach Virtual Network)**」をクリックして、使用可能な仮想ネットワークを表示し、論理区画に追加の仮想ネットワークを接続することができます。

選択した区画の仮想ネットワークを、HMC を使用して表示するには、以下のステップを実行します。

- ナビゲーション領域で、リソース・アイコン  をクリックしてから、「すべてのパーティション」を選択します。
- 保守容易性タスクを管理する区画を選択して、「アクション」 > 「区画属性の表示」をクリックします。
- メニュー・ポッドで、「仮想 I/O」を展開し、さらに、「仮想ネットワーク」をクリックします。

このタスクについて詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

仮想 NIC

クライアント区画に関連付けられている仮想ネットワーク・インターフェース・コントローラー (NIC) 構成のすべての特性を管理することができます。

仮想 NIC とは、ネットワーク・インターフェースを提供するために論理区画上で構成できる一種の仮想アダプターです。各仮想 NIC クライアント・アダプターは、ホスティング区画で所有されている SR-IOV 論理ポートでバックアップされます。

仮想 NIC テーブルには、選択された区画用に構成されている仮想 NIC がすべてリストされます。仮想 NIC は 1 つ以上のバックアップ・デバイスを持つことができます。仮想 NIC 1 つあたりの最大バックアップ・デバイス数はシステムによって異なります。仮想 NIC に複数のバックアップ・デバイスがある場合は、ノードを展開してすべてのバックアップ・デバイスを表示できます。仮想 NIC にあるバックアップ・デバイスが 1 つのみの場合は、そのバックアップ・デバイスがアクティブ・バックアップ・デバイスとなります。アクティブ・バックアップ・デバイスとは、仮想 NIC で使用中のバックアップ・デバイスのことです。管理対象システムがフェイルオーバーに対応していない場合は、単一のバックアップ・デバイスを持つ仮想 NIC がテーブルに表示されます。

仮想 NIC は区画に追加できます。仮想 NIC を追加するには、「**仮想 NIC の追加**」をクリックします。仮想 NIC を構成できるのは、専用モードでのみです。仮想 NIC の属性を変更したり表示したりすることもできます。仮想 NIC の属性を変更するには、テーブルで仮想 NIC を選択し、「**アクション**」>「**vNIC の変更**」をクリックします。仮想 NIC の属性を表示するには、テーブルで仮想 NIC を選択し、「**アクション**」>「**vNIC の表示**」をクリックします。

選択した区画の仮想 NIC を、HMC を使用して表示するには、以下のステップを実行します。



1. ナビゲーション領域で、**リソース・アイコン** をクリックしてから、「**すべてのパーティション**」を選択します。
2. 保守容易性タスクを管理する区画を選択して、「**アクション**」>「**区画属性の表示**」をクリックします。
3. メニュー・ポッドで、「**仮想 I/O**」を展開してから、「**仮想 NIC**」をクリックします。

このタスクについて詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

仮想ストレージ

論理区画のストレージ機能を作成、表示、および管理することができます。

「**仮想ストレージ**」テーブルに、論理区画に対して構成されている仮想 Virtual Small Computer Serial Interface (SCSI) デバイスが表示されます。物理ボリューム・グループ、共用ストレージ・プール・ボリューム、および論理ボリュームに関する情報も表示できます。

仮想ストレージ・リソースを区画に追加できます。論理区画について割り当てられている仮想ストレージ・デバイスのアダプター 構成を作成したり表示したりするには、「**アダプター・ビュー**」をクリックします。論理区画のストレージ機能を表示および管理するには、「**ストレージ・ビュー**」をクリックします。

物理ボリュームは、仮想 SCSI ディスクとして区画にエクスポートすることができます。論理区画に既に割り当てられている割り当て済みの物理ボリュームを表示するには、「**割り当て済みの物理ボリュームを表示**」をクリックします。

物理ボリュームを区画に追加するには、リストから物理ボリュームを選択し、区画に追加する物理ボリュームごとに「**ユーザー定義名**」を指定して、「**了解**」をクリックします。各物理ボリュームに割り当てられているサーバー・アダプター ID を変更したい場合は、更新したい物理ボリュームのそれぞれについて「**編集**」をクリックします。「**接続の編集**」ウィンドウが表示されます。最大 3 つの Virtual I/O Server を指定し、アダプター接続用に割り当てる新規サーバー・アダプター ID を入力することができます。

異なるタイプの仮想ストレージ・デバイスを区画に追加するには、「**仮想 SCSI デバイスの追加**」をクリックします。追加する、使用可能な仮想ストレージを選択します。仮想ストレージ・タイプ (物理ボリューム、共用ストレージ・プール・ボリューム、論理ボリュームなど) を選択できます。

選択した区画の仮想ストレージを、HMC を使用して表示するには、以下のステップを実行します。



1. ナビゲーション領域で、**リソース・アイコン** をクリックしてから、「**すべてのパーティション**」を選択します。
2. 保守容易性タスクを管理する区画を選択して、「**アクション**」>「**区画属性の表示**」をクリックします。
3. メニュー・ポッドで、「**仮想 I/O**」を展開してから、「**仮想ストレージ**」をクリックします。

このタスクについて詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

ハードウェア仮想化 I/O

ハードウェア管理コンソール (HMC) を使用して、区画のシングル・ルート I/O 仮想化 (SR-IOV) ポート・アダプターや論理ホスト・イーサネット・アダプター (LHEA) など、ハードウェア仮想化 I/O アダプターの設定を表示および変更できます。

選択した区画のハードウェア仮想化 I/O アダプターを、HMC を使用して表示するには、以下のステップを実行します。



1. ナビゲーション領域で、リソース・アイコン  をクリックしてから、「すべてのパーティション」を選択します。
2. 保守容易性タスクを管理する区画を選択して、「アクション」>「区画属性の表示」をクリックします。
3. メニュー・ポッドで、「仮想 I/O」を展開し、さらに、「ハードウェア I/O」をクリックします。
4. 「SRIOV」タブで、SR-IOV 論理ポートを区画に追加したり、SR-IOV 論理ポートの設定を変更したりすることができます。「SR-IOV 論理ポート」表では、移行可能な論理ポートに関する情報と、論理ポート用に構成されているバックアップ・デバイスに関する情報を表示することもできます。「論理ホスト・イーサネット・アダプター」(LHEA) タブで、LHEA アダプターの設定を変更できます。LHEA アダプターを追加したり除去したりすることもできます。

注：

- HMC バージョン 9.1.930 以降では、HMC は RDMA over Converged Ethernet (RoCE) アダプターもサポートします。
- HMC バージョン 9.1.940 を使用していて、ファームウェアがレベル FW940 以降である場合、移行可能な SR-IOV 論理ポートを持つ論理区画を作成できます。論理ポートの作成時にバックアップ仮想デバイスを作成するために「移行可能」オプションが使用されている場合、SR-IOV 論理ポートを持つ論理区画を移行できます。バックアップ・デバイスは、仮想イーサネット・アダプターまたは仮想ネットワーク・インターフェース (NIC) アダプターにすることができます。HMC がバージョン 9.1.940.x であり、かつファームウェアがレベル FW940 の場合、Hybrid Network Virtualization 機能の「移行可能」オプションは、テクノロジー・プレビューとしてのみ使用でき、実動でのデプロイメントは意図されていません。ただし、HMC がバージョン 9.1.941.0 以降であり、ファームウェアがレベル FW940.10 以降の場合は、Hybrid Network Virtualization 機能の「移行可能」オプションはサポートされます。

このタスクについて詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

システム管理 (フレーム)

フレームのセットアップ、構成、状態の表示、トラブルシューティング、および解決策の適用を行います。

属性

選択したフレーム属性を表示します。

フレーム属性には、以下の属性があります。

一般

「一般」タブは、フレームの名前と番号、状態、タイプ、モデル、およびシリアル番号を表示します。

管理対象システム

「管理対象システム」タブは、フレームに含まれているすべての管理対象システムおよびそのケージ番号を表示します。ケージとは、管理対象システム、I/O ユニット、および大容量電源アセンブリー (BPA) を保持するエンクロージャーの区分です。

I/O ユニット

「I/O ユニット」タブは、フレームに含まれているすべての I/O ユニット、それらのケージ番号、およびそれらが割り当てられた管理対象システムを表示します。ケージとは、管理対象システム、I/O ユニット、および BPA を保持するエンクロージャーの区分です。「システム」の列に「非所有 (Not owned)」とあるものは、対応する I/O ユニットが管理対象システムに割り当てられていないことを表します。

操作

管理対象フレームで、タスクを実行します。

フレームの初期化

管理対象フレームの初期化方法について説明します。

この操作タスクは、1つ以上のフレームを選択した場合にのみ使用できます。このタスクでは、最初に、選択された管理対象フレーム内の未所有の I/O ユニットの電源がオンにされ、次に、選択された管理対象フレーム内の管理対象システムの電源がオンにされます。完全な初期化プロセスが完了するまで数分かかる場合があります。

注: 既に電源がオンになっている管理対象システムは、影響を受けません。電源がオフになって再度オンになることはありません。

全フレームの初期化

すべてのフレームを初期化します。

このタスクについて

この操作タスクは、管理対象フレームが選択されておらず、しかも、ナビゲーション領域の「フレーム」タブが強調表示されている場合に使用できます。このタスクでは、最初に、各管理対象フレーム内の未所有の I/O ユニットの電源がオンにされ、次に、各管理対象フレーム内の管理対象システムの電源がオンにされます。

注: フレームが HMC に接続されている場合は、既に電源オンになっています。フレームを初期化してもフレームの電源はオンになりません。

再ビルド

ハードウェア管理コンソール (HMC) インターフェースでフレーム情報を更新します。

フレームの更新または再ビルドの動作は、フレーム情報の最新表示と非常に似ています。フレームの再ビルドは、HMC の作業ペインのシステムの状態インディケーターに **Incomplete** (不完全) が表示されたときに役立ちます。「**Incomplete**」(不完全) インディケーターは、HMC がフレーム内の管理対象システムから完全なリソース情報を収集できないことを示します。

このプロセス中に HMC で他のタスクを実行することはできません。このプロセスは数分かかる場合があります。

パスワードの変更

選択した管理対象フレームに対するハードウェア管理コンソール (HMC) アクセス・パスワードを変更します。

パスワードを変更したら、この管理対象フレームにアクセスする他のすべての HMC について HMC アクセス・パスワードを更新する必要があります。

現在のパスワードを入力してから、新しいパスワードを入力し、検証のために新しいパスワードを再度入力してください。

I/O ユニットの電源オン/オフ

ハードウェア管理コンソール (HMC) インターフェースを使用して、I/O ユニットの電源をオフにします。

電源ドメインにあるユニットまたはスロットのみ、電源オフにできます。対応する電源オン/オフ・ボタンは、HMC から制御できないロケーション・コードに対しては使用不可になります。

構成

「構成」タスクを使用して、フレームを構成することができます。「構成」タスクを使用してカスタム・グループも管理できます。

カスタム・グループの管理

状況をグループ別にレポートすることによって、選択した方法でシステムをモニターできます。

グループはネストもできる (グループ内にグループを含める) ため、階層表示またはトポロジー表示ができます。

すでに 1 つ以上のユーザー定義グループが、ご使用の HMC に定義されている可能性があります。デフォルト・グループは、「サーバー管理」の下の「カスタム・グループ」ノードの下にリストされます。デフォルト・グループは、「すべての区画」と「すべてのオブジェクト」です。「カスタム・グループの管理」タスクを使用して、他のグループを作成したり、作成したグループを削除、作成したグループにグループを追加、パターン・マッチング方式を使用してグループを作成、または作成したグループからグループを削除することができます。

グループの操作について詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

接続

「接続」タスクを使用して、フレームへのハードウェア管理コンソール (HMC) 接続の状況を表示したり、それらの接続をリセットしたりすることができます。

大容量電源アセンブリー (BPA) の状況

「大容量電源アセンブリー (BPA) の状況」タスクを使用して、ハードウェア管理コンソール (HMC) から大容量電源アセンブリーのサイド A およびサイド B への接続の状態を表示します。HMC はサイド A またはサイド B のいずれかに接続することによって正常に作動しますが、コードの更新操作および一部の並行保守操作では、HMC は両サイドに接続する必要があります。

HMC には、以下の情報が表示されます。

- IP アドレス (IP address)
- BPA ロール
- 接続状況
- 接続エラー・コード

状況が「接続されていない」の場合、接続状況は次のいずれかの条件になります。

開始中/不明

フレーム内の大容量電源アセンブリー (BPA) の 1 つが始動中です。別の BPA の状態は不明です。

スタンバイ/スタンバイ

フレーム内に含まれる BPA が両方ともスタンバイ状態にあります。「スタンバイ」状態にある BPA は、正常な作動をしています。

スタンバイ/開始中

フレーム内に含まれる BPA の一方が正常に作動しています (スタンバイ状態)。反対側の BPA は開始プロセス中です。

スタンバイ/使用不可

フレーム内に含まれる BPA の一方は、正常に作動していますが (スタンバイ状態)、もう一方の BPA が正常に作動していません。

保留フレーム番号

フレーム番号の変更を処理中です。フレームがこの状態にある場合、操作は完了されません。

認証に失敗

フレームに対する HMC のアクセス・パスワードが有効ではありません。フレームに対して有効なパスワードを入力します。

認証は保留中 - パスワードの更新が必要です

フレームのアクセス・パスワードが設定されていません。フレームに対して必要なパスワードを設定して、セキュアな認証と HMC からのアクセス制御を可能にする必要があります。

接続なし

HMC はフレームに接続できません。

不完全

HMC は管理対象フレームから必要なすべての情報を入手することに失敗しました。情報の要求に対してフレームは応答しません。

リセット

ハードウェア管理コンソール (HMC) と選択した管理対象フレームのとの間の接続をリセットします。

管理対象フレームとの接続をリセットすると、接続は切断されてから再接続されます。管理対象フレームが「接続なし」状態であり、HMC と管理対象フレームの両方においてネットワークの設定値が正しいことを確認したら、管理対象フレームとの接続をリセットしてください。

保守容易性

ハードウェア管理コンソール (HMC) の問題分析によって、エラー条件が自動的に検出され、修復サービスが必要な問題が報告されます。

これらの問題は、サービス可能イベントとして報告されます。選択したシステムの特定のイベントを表示して、現場交換可能ユニット (FRU) を追加、除去、または交換することができます。「サービス可能イベント・マネージャー」タスクを使用して、選択したフレームの特定のイベントを表示します。

ご使用のフレームに使用可能な保守容易性タスクを開くには、以下の手順を実行します。

1. ナビゲーション領域で、リソース・アイコン  をクリックしてから、「すべてのフレーム」を選択します。
2. 保守容易性タスクを管理したいフレームを選択します。
3. メニュー・ポッドで、「保守容易性」を展開してから、「保守容易性」をクリックします。
4. 実行する保守容易性タスクをリストから選択します。

サービス可能イベント・マネージャー

管理対象フレーム上の問題は、ハードウェア管理コンソール (HMC) にサービス可能イベントとして報告されます。問題の表示、問題データの管理、サービス・プロバイダーへのイベントのコール・ホーム、または問題の修理が可能です。

表示するサービス可能イベントの基準を設定するには、以下の手順を実行します。

1. メニュー・ポッドから、「サービス可能イベント・マネージャー」を開きます。
2. イベント基準、エラー基準、および FRU 基準を指定します。
3. 「了解」をクリックします。
4. フィルタリングされた結果を必要としない場合は、「すべて」を選択します。

「サービス可能イベントの概要」ウィンドウは、基準と一致するすべてのイベントを表示します。短縮テーブル・ビューに表示される情報には、以下のフィールドが含まれています。

- 問題番号。
- PMH 番号。
- 参照コード: 「参照」コードをクリックして、問題の修正に使用できる問題報告およびアクションの説明を表示します。
- 問題の状況。
- 問題の最終報告時間。

- 問題によって障害の起きた MTMS。

表のすべてを表示すると、報告された MTMS、最初の報告時間、およびサービス可能イベントのテキストなど、より詳細な情報が含まれます。

サービス可能イベントを選択し、以下の作業を実行します。

- **イベント詳細の表示 (View event details):** このイベントに関連する FRU とその説明を表示します。
- **イベントの修復 (Repair the event):** 使用可能ならガイド付き修理手順を開始します。
- **イベントのコール・ホーム (Call home the event):** イベントをサービス・プロバイダーに報告します。
- **イベント問題データの管理 (Manage event problem data):** データおよびこのイベントに関連するログを表示、コール・ホーム、またはメディアにオフロードします。
- **イベントを閉じる (Close the event):** 問題の解決後、コメントを追加してイベントを閉じます。

サービス可能イベントの管理について詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

ハードウェア

これらのタスクを使用すると、管理対象フレームについてハードウェアを追加、交換、または除去できます。「ハードウェア」タスクから、インストール済みの FRU またはエンクロージャー、およびそれらのロケーションのリストを表示できます。FRU またはエンクロージャーを選択して、その装置を追加、交換、または除去するステップバイステップの手順を開始します。

FRU の追加

「**FRU の追加**」タスクを使用し、FRU の位置を見つけて追加します。

FRU を追加するには、以下の手順を実行します。

1. 「**FRU**」メニューで、エンクロージャー・タイプを選択します。
2. FRU のタイプを選択します。
3. 「**次へ**」をクリックします。
4. ロケーション・コードを選択します。
5. 「**追加**」をクリックして、選択したエンクロージャーのロケーションを「**保留アクション**」に追加します。
6. 「**プロシーチャーの起動**」をクリックして、選択した FRU タイプを「**保留アクション**」で指定したエンクロージャーのロケーションに追加します。
7. FRU のインストール・プロセスが完了したら、「**完了**」をクリックします。

エンクロージャーの追加

「**エンクロージャーの追加**」タスクを使用して、エンクロージャーの位置を指定して追加します。

エンクロージャーを追加するには、以下の手順を実行します。

1. エンクロージャー・タイプを選択してから、「**追加**」をクリックして選択したエンクロージャー・タイプのロケーション・コードを「**保留アクション**」に追加します。
2. 「**保留アクション**」で指定したエンクロージャーを、選択したシステムに追加するには、「**プロシーチャーの起動**」をクリックします。
3. エンクロージャーのインストール・プロセスが完了したら、「**完了**」をクリックします。

FRU の交換

FRU を別の FRU に交換します。

FRU を交換するには、以下の手順を実行します。

1. インストールされたエンクロージャーのタイプを選択します。
2. FRU のタイプを選択します。
3. 「**次へ**」をクリックします。

4. 特定の FRU のロケーション・コードを選択します。
5. 「追加」をクリックする。
6. 「**プロシーチャーの起動**」を選択します。

注：この手順では、「**FRU の交換**」タスクの影響を受けるリソース (区画が使用中のすべてのリソースを含む) を識別します。冗長性が構成されていない場合には、区画で実行中のワークロードに影響が及ぶ可能性があります。画面上の指示に従って、交換を完了します。

7. インストールが完了したら、「完了」をクリックします。

エンクロージャの交換

エンクロージャを別のエンクロージャに交換します。

エンクロージャを交換するには、以下の手順を実行します。

1. インストール済みのエンクロージャを選択してから、「追加」をクリックして、選択したエンクロージャのロケーション・コードを「**保留アクション**」に追加します。
2. 「**プロシーチャーの起動**」をクリックし、選択したシステムにおいて「**保留アクション**」で指定したエンクロージャの置換を開始します。
3. エンクロージャの交換プロセスが完了したら、「完了」をクリックします。

FRU の除去

管理対象システムから FRU を除去します。

FRU を取り外すには、以下の手順を実行します。

1. メニューからエンクロージャを選択します。
2. このエンクロージャについて表示された FRU タイプのリストから、FRU のタイプを選択します。
3. 「次へ」をクリックします。
4. 特定の FRU のロケーション・コードを選択します。
5. 「追加」をクリックする。
6. 「**プロシーチャーの起動**」を選択します。
7. 除去手順が完了したら、「完了」をクリックします。

エンクロージャの除去

ハードウェア管理コンソール (HMC) が指定するエンクロージャを除去します。

エンクロージャを取り外すには、以下の手順を実行します。

1. エンクロージャ・タイプを選択し、「追加」をクリックします。
2. 「**プロシーチャーの起動**」をクリックします。
3. エンクロージャの除去プロセスが完了したら、「完了」をクリックします。

グループの管理

「すべてのグループ」ビューには、システム・リソースをグループ化して単一ビューにまとめるメカニズムが備わっています。

グループをネストして、カスタマイズされたシステム・リソース・ビューを作成できます。

グループ内のシステム・リソースに関する累積状態情報を含め、管理コンソールのユーザーによって作成されたすべてのグループを表示することができます。カスタム・グループは、管理コンソールによって管理される任意のシステム、区画、および Virtual I/O Server で構成することができます。

新規グループを作成するには、以下の手順を実行します。

1. ツールバーで「**グループの作成 (Create group)**」をクリックします。
2. 「**グループの作成 (Create group)**」ウィンドウで、グループの名前と説明を指定します。作成するグループに色でタグ付けすることができます。

3. 作業の対象としてグループに含める 1 つ以上のリソース (サーバー、区画、またはフレームなど) を選択します。
4. 「OK」をクリックして変更を保管し、ウィンドウを閉じます。

既存のグループを編集して、グループのリソースを追加したり削除したりすることができます。

注: グループの最後のメンバー (リソース) が削除されると、グループを削除するかどうかを確認するメッセージが表示されます。「すべてのグループ」ビューにグループを残す場合は、「取消」をクリックします。

Power エンタープライズ・プール

Power エンタープライズ・プールのシステム管理は、実行することができる Power エンタープライズ・プールのタスクを表示します。

Power エンタープライズ・プールのオフファリングを使用して、以下の操作を実行することができます。

- サーバーにプロセッサまたはメモリーを追加する。
- サーバーからプロセッサまたはメモリーを除去する。
- プール構成を更新する。
- プールにサーバーを追加する。
- プールから既存のサーバーを除去する。
- プールにプロセッサまたはメモリーを追加する。
- 以下の Power エンタープライズ・プール 情報を表示する
 - プール・メンバーシップ情報
 - プール・リソース情報
 - プール・コンプライアンス情報
 - プール・ヒストリー・ログ

HMC 管理タスク

ハードウェア管理コンソール (HMC) の「**HMC 管理**」で使用可能なタスクについて説明します。

タスクを開く方法については、9 ページの『[HMC タスク、ユーザー・ロール、ID、および関連コマンド](#)』を参照してください。

注: ユーザー ID に割り当てられたタスク・ロールに応じて、すべてのタスクにはアクセスできない場合があります。タスクとそれらのタスクにアクセス可能なユーザー・ロールのリストは、9 ページの表 3 を参照してください。

ガイド付きセットアップ・ウィザードの起動

このタスクはウィザードを使用して、システムおよび HMC をセットアップします。



1. ナビゲーション領域で、**HMC 管理**アイコン  をクリックしてから、「**コンソール設定**」を選択します。
2. コンテンツ・ペインで、「**ガイド付きセットアップ・ウィザードの起動**」をクリックする。
3. 「**ガイド付きセットアップ・ウィザードの起動 - ようこそ**」ウィンドウから、特定の前提条件を用意しておくことをお勧めします。情報を得るには、「**ガイド付きセットアップ・ウィザードの起動 - ようこそ**」ウィンドウの「**前提条件**」をクリックします。この操作を完了したら、ウィザードに従ってシステムと HMC のセットアップに必要な以下のタスクを実行します。それぞれのタスクを完了するたびに「**次へ**」をクリックして先に進みます。

- a. HMC 日付と時刻の変更
 - b. HMC パスワードの変更
 - c. 追加の HMC ユーザーの作成
 - d. HMC ネットワーク設定の構成 (このタスクは、「ガイド付きセットアップ・ウィザードの起動」にリモート側でアクセスしている場合は実行できません)
 - e. 連絡先情報の指定
 - f. 接続情報の構成
 - g. ユーザーに Electronic Service Agent ソフトウェア・ツールの使用を許可して、問題イベントの通知を構成します。
4. ウィザードのすべてのタスクを完了したら「完了」をクリックします。

ネットワーク・トポロジーの表示

このタスクにより、ハードウェア管理コンソール (HMC) 内の各種ネットワーク・ノード間の接続性を表示および ping することができます。

ネットワーク・トポロジーを表示するには、以下の手順を実行します。

1. ナビゲーション領域で、**HMC 管理アイコン**  をクリックしてから、「**コンソール設定**」を選択します。
2. コンテンツ・ペインで、「**ネットワーク・トポロジーの表示**」をクリックします。
3. 「**ネットワーク・トポロジーの表示**」ウィンドウから、現行ノードおよび保管済みノードを ping することができます。s
4. このタスクを終了したら、「**クローズ**」をクリックします。

ネットワーク・トポロジーの表示に関する詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

ネットワーク接続性のテスト

このタスクにより、ハードウェア管理コンソール (HMC) のネットワーク・プロトコルに関するネットワーク診断情報を表示することができます。

ネットワーク接続性をテストするには、以下のステップを実行します。

1. ナビゲーション領域で、**HMC 管理アイコン**  をクリックしてから、「**コンソール設定**」を選択します。
2. コンテンツ・ペインで、「**ネットワーク接続性のテスト**」をクリックします。
3. 「**ネットワーク接続性のテスト**」ウィンドウでは以下のタブを使用できます。

Ping

TCP/IP アドレスまたは名前を ping できます。

インターフェース

現在構成済みのネットワーク・インターフェースの統計を表示します。最新情報と一緒に現在表示されている情報を更新するには、「**最新表示**」をクリックします。

イーサネット設定

現在構成済みのイーサネット・カードの設定を表示します。最新情報と一緒に現在表示されている情報を更新するには、「**最新表示**」をクリックします。

アドレス

構成済みのネットワーク・インターフェースの TCP/IP アドレスを表示します。最新情報と一緒に現在表示されている情報を更新するには、「**最新表示**」をクリックします。

経路

カーネル IP および IPv6 のルーティング・テーブルと対応するネットワーク・インターフェースを表示します。最新情報と一緒に現在表示されている情報を更新するには、「**最新表示**」をクリックします。

ARP

アドレス解決プロトコル (ARP) 接続のコンテンツを表示します。最新情報と一緒に現在表示されている情報を更新するには、「**最新表示**」をクリックします。

ソケット

TCP/IP ソケットに関する情報を表示します。最新情報と一緒に現在表示されている情報を更新するには、「**最新表示**」をクリックします。

TCP

伝送制御プロトコル (TCP) 接続に関する情報を表示します。最新情報と一緒に現在表示されている情報を更新するには、「**最新表示**」をクリックします。

IP テーブル

インターネット・プロトコル (IP) パケット・フィルタ・ルールに関する情報を (表形式で) 表示します。最新情報と一緒に現在表示されている情報を更新するには、「**最新表示**」をクリックします。

UDP

User Datagram Protocol (UDP) 統計に関する情報を表示します。最新情報と一緒に現在表示されている情報を更新するには、「**最新表示**」をクリックします。

4. タスクを完了したら「**取消**」をクリックします。

ネットワーク接続性のテストに関する詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

ネットワーク設定の変更

このタスクを使用して、HMC に関する現在のネットワーク情報を表示したり、ネットワークの設定に変更を加えたりします。



1. ナビゲーション領域で、**HMC 管理**アイコン  をクリックしてから、「**コンソール設定**」を選択します。
2. コンテンツ・ペインで、「**ネットワーク設定の変更**」をクリックします。
3. 「**ネットワーク設定の変更**」ウィンドウでは以下のタブを使用できます。

識別

HMC のホスト名、ドメイン・ネーム、およびコンソールの説明が含まれます。

LAN アダプター

すべての (可視の) Local Area Network (LAN) アダプターの要約リストです。これらのいずれかを選択して「**詳細...**」をクリックするとウィンドウが開き、アドレス指定、経路指定、他の LAN アダプターの特性、およびファイアウォール設定を変更できます。

Bond LAN アダプター

Bond LAN アダプターを作成または削除します。Bond LAN アダプターは、2つのイーサネット・インターフェースを結合して単一の論理リンクにします。Bond LAN アダプターの設定を変更するには、Bond LAN アダプターを選択し、「**編集**」をクリックします。Bond LAN アダプターの IP アドレス、IP ネットワーク・マスク、ゲートウェイ、およびファイアウォールの設定を変更することができます。

ネーム・サービス

コンソールのネットワーク設定を構成するために、DNS 値およびドメイン・サフィックス値を指定します。

経路指定

コンソールのネットワーク設定の構成に使用する経路指定情報およびデフォルトのゲートウェイ情報を指定します。

ゲートウェイ・アドレスは、すべてのネットワークへの経路です。デフォルトのゲートウェイ・アドレス (定義されている場合) は、ターゲット・ステーションがソースと同じサブネット上でない場合のデータの送信先をこの HMC に通知します。ご使用のマシンと同じサブネット上 (通常は建物または建物内の部門) のどのステーションにも送信できるがその領域外との通信を行えない場合は、たいていはデフォルト・ゲートウェイの構成が正しくないことがその原因です。

特定の LAN を **ゲートウェイ・デバイス** として割り当てるか、「任意 (any)」を選択できます。

「**RouteD を使用可能にする (Enable 'routed')**」を選択してルート・デーモンを始動することができます。これによって、ルート・デーモンを実行し、経路指定情報を HMC からエクスポートできます。

4. このタスクを終了したら、「**了解**」をクリックします。

注: 加えた変更のタイプによって、ネットワークまたはコンソールが自動的に再始動するか、コンソールが自動的にリブートします。

ネットワーク設定のカスタマイズの詳細については、オンライン・ヘルプを利用してください。

パフォーマンス・モニター設定の変更

「パフォーマンスと容量のモニター」ツールは、仮想化されたサーバー・リソースの割り振りデータおよび使用量データを収集します。また、データをグラフおよびテーブルの形式で表示します。これは「パフォーマンスと容量のモニター」のホーム・ページから参照できます。

「パフォーマンスと容量のモニター」はデータを収集し、容量のレポートとパフォーマンスのモニターを可能にします。この情報は使用可能な容量を調べて、使用している容量が過剰か、基準以下であるかの判別に役立ちます。さらに、グラフまたは表に変換処理すると、キャパシティ・プランニングおよびトラブルシューティングで役に立ちます。「パフォーマンスと容量のモニター」ツールについて詳しくは、[パフォーマンスと容量のモニターの使用](#)を参照してください。

「パフォーマンスと容量のモニター」は、データ収集を可能にするために選択するサーバーからのみデータを取り込みます。

データ収集を使用可能にするには、以下の手順を完了します。



1. ナビゲーション領域で、**HMC 管理アイコン** をクリックしてから、「**コンソール設定**」を選択します。
2. コンテンツ・ペインで、「**パフォーマンス・モニター設定の変更**」をクリックします。
3. 1 から 366 の数を入力して、パフォーマンス・データを保管する 日数を指定します。別の方法として、「**パフォーマンス・データ・ストレージ (Performance Data Storage)**」の下で「**パフォーマンス・データ保管日数 (Number of days to store performance data)**」の横にある上矢印または下矢印をクリックすることもできます。

注: HMC はデフォルトで、データを 180 日間保管します。ただし、HMC がデータを保管する最大日数を 366 日間に指定できます。

4. データを収集するサーバーの名前の横にある「**収集 (Collection)**」列で、切り替えスイッチをクリックします。別の方法として、「**すべてオン (All On)**」をクリックして、HMC で管理する環境内のすべてのサーバーについてデータ収集を使用可能にすることもできます。

注: ストレージ・スペースの制限により、ご使用の環境のすべてのサーバーからデータを収集できないことがあります。予定のストレージ・スペースを使い尽くしたと HMC が判断した場合、HMC はユーザーがその後のサーバーからデータを収集できないようにします。

5. 「**了解**」をクリックして変更内容を適用し、ウィンドウを閉じます。これで、「パフォーマンスと容量のモニター」のホーム・ページにアクセスして収集したデータをレビューできるようになりました。

日付と時刻の変更

バッテリー駆動のハードウェア管理コンソール (HMC) クロックの日時の変更、および Network Time Protocol (NTP) サービスのタイム・サーバーの追加または除去を行います。

このタスクは、次のような場合に使用します。

- HMC でバッテリーが交換された場合。
- システムが物理的に別の時間帯に移動された場合。

注: 選択したタイム・ゾーンで夏時間調整が行われている場合、時刻設定は自動的に調整されます。

日時を変更するには、次の手順を完了します。

1. ナビゲーション領域で、**HMC 管理アイコン**  をクリックしてから、「**コンソール設定**」を選択します。
2. 「コンテンツ」ペインで、「**日付/時刻の変更**」をクリックします。
3. 「**コンソール日付/時刻のカスタマイズ**」タブをクリックします。
4. 日時の情報を入力します。
5. 「**了解**」をクリックします。

タイム・サーバー情報を変更するには、以下の手順を完了します。

1. ナビゲーション領域で、**HMC 管理アイコン**  をクリックしてから、「**コンソール設定**」を選択します。
2. 「コンテンツ」ペインで、「**日付/時刻の変更**」をクリックします。
3. 「**NTP 構成**」タブをクリックします。
4. タイム・サーバーの該当する情報を入力します。
5. 「**了解**」をクリックします。

HMC の日時の変更に関する詳細情報、または Network Time Protocol (NTP) サービスへのタイム・サーバーの追加または除去に関する詳細情報が必要な場合は、オンライン・ヘルプを使用してください。

言語およびロケールの変更

このタスクは HMC の言語および場所を設定します。言語を選択した後、その言語に関連するロケールを選択できます。

言語およびロケールの設定により、言語、文字セット、および国または地域に固有のその他の設定 (例えば日付、時刻、数値の形式、通貨単位など) が決まります。「**言語およびロケールの変更**」ウィンドウで行われた変更は、HMC 自体の言語およびロケールにのみ影響します。リモート側から HMC にアクセスしている場合、ブラウザ上の言語およびロケールの設定により、ブラウザが HMC インターフェースを表示するために使用する設定が決まります。

HMC の言語およびロケールを変更する場合:

1. ナビゲーション領域で、**HMC 管理アイコン**  をクリックしてから、「**コンソール設定**」を選択します。
2. コンテンツ・ペインで、「**言語およびロケールの変更**」をクリックします。
3. 「**言語およびロケールの変更**」ウィンドウから該当する言語およびロケールを選択します。
4. 「**了解**」をクリックして変更を適用します。

HMC の言語およびロケールの変更について詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

ようこそテキストの作成

ユーザーがハードウェア管理コンソール (HMC) にログオンする前に表示されるようこそメッセージの作成および表示、または警告メッセージの表示を行います。

このタスクのメッセージ入力域に入力したテキストは、最初にコンソールにアクセスした後に出される「ようこそ」ウィンドウに表示されます。このテキストを使用して、ユーザーに特定の企業ポリシーやシステムに適用するセキュリティ制限について通知できます。

ようこそテキストを作成するには、以下の手順を実行します。



1. ナビゲーション領域で、**HMC 管理アイコン** をクリックしてから、「**コンソール設定**」を選択します。
2. コンテンツ・ペインで、「**ウェルカム・テキストの作成**」をクリックします。
3. 表示したいようこそテキストをテキスト・ボックスに入力します。

注：最大で 8192 文字を使用できます。

4. 「**了解**」をクリックします。

このタスクについての詳細は、オンライン・ヘルプを使用します。

コンソールのデフォルト設定

ハードウェア管理コンソール (HMC) でデフォルトのコンソール設定を変更することができます。

また、証明書が有効な日数を変更することもできます。

注：証明書を有効にすることができる期間は、最大で 3650 日です、

コンソールのデフォルト設定を変更するには、以下のステップを実行します。



1. ナビゲーション領域で、**HMC 管理アイコン** をクリックしてから、「**コンソール設定**」を選択します。
2. コンテンツ・ペインで、「**コンソールのデフォルト設定 (Console Default Settings)**」をクリックします。
3. 「**コンソール・デフォルト設定**」ウィンドウでは、証明書が有効になる日数を指定できるほか、HMC セッションのタイムアウト設定を構成することもできます。HMC 9.1.940 以降を使用している場合、HMC グラフィカル・ユーザー・インターフェース (GUI) へのログイン試行の最大回数を指定できます。3 から 50 の範囲の値を入力することができます。
4. タスクが完了したら、「**了解**」をクリックします。

このタスクについて詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

シャットダウンまたは再始動

このタスクは、コンソールのシャットダウン (コンソールの電源をオフ) または再始動を可能にします。



1. ナビゲーション領域で、**HMC 管理アイコン** をクリックしてから、「**コンソール管理**」を選択します。
2. コンテンツ・ペインで、「**シャットダウンまたは再始動**」をクリックします。
3. 「**シャットダウンまたは再始動**」ウィンドウでは以下の処理ができます。

- 「**HMC の再始動 (Restart the HMC)**」を選択して、シャットダウンが起きた HMC を自動的に再始動します。

- HMC を自動的に再始動しない場合は、「**HMC の再始動**」を選択しないでください。
4. 「**了解**」をクリックしてシャットダウンを続行します。続行しない場合は、「**取消**」をクリックしてタスクを終了します。
- HMC のシャットダウンまたは再始動について詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

操作のスケジュール

特定の操作がオペレーターの介入なしでハードウェア管理コンソール (HMC) で自動的に実行されるように、スケジュールを作成します。

システム 操作の自動処理、遅延処理、または反復処理が必要な状況では、スケジュール操作が便利です。スケジュール操作は、指定した時刻に、オペレーターが操作の実行に携わることなく開始します。スケジュールには、1 回の操作または複数回の繰り返しを設定できます。

例えば、DVD への重要な HMC 情報のバックアップを一度だけ行うようにスケジュールしたり、繰り返しスケジュールをセットアップしたりできます。

「**スケジュール操作**」タスクは、各操作について次の情報を表示します。

- 操作の対象になるプロセッサ
- スケジュールされている日付
- スケジュールされている時刻
- 操作
- 残されている繰り返し回数

「**スケジュール操作**」ウィンドウでは以下の処理ができます。

- 操作を後で実行するようスケジュールします。
- 操作を定期的な間隔で繰り返し実行するように定義します。
- スケジュール操作を削除します。
- 現在スケジュールされている操作の詳細を表示します。
- 指定した時刻範囲内にスケジュールされている操作を表示します。
- スケジュールされている操作を、日付、操作、または管理対象システム別にソートします。

操作は 1 回実行するように、または繰り返し実行されるようにスケジュールできます。操作が実行される時刻および日付を指定する必要があります。操作が繰り返し実行されるようにスケジュールされている場合、以下について選択する必要があります。

- 操作を実行する曜日 (任意)
- 操作の実行間隔または時刻 (必須)
- 繰り返しの合計回数 (必須)

HMC についてスケジュールできる操作は次のとおりです。

重要なコンソール・データのバックアップ

HMC の重要なコンソール・ハード・ディスク情報をバックアップする操作をスケジュールします。

HMC 上の操作をスケジュールするには、以下のステップを完了します。



1. ナビゲーション領域で、**HMC 管理**アイコンをクリックしてから、「**コンソール管理**」を選択します。
2. コンテンツ・ペインで、「**操作のスケジュール**」をクリックします。
3. 「**操作をスケジュールする**」ウィンドウでメニューバーの「**オプション**」をクリックして、次のレベルのオプションを表示します。
 - スケジュール操作を追加するには、「**オプション**」を選択してから「**新規**」をクリックします。

- スケジュール操作を削除するには、削除する操作を選択して「**オプション**」を選択してから「**削除**」をクリックします。
 - 選択したオブジェクトについて、スケジュール操作のリストを現在のスケジュールで更新するには、「**オプション**」を選択してから「**最新表示**」をクリックします。
 - スケジュール操作を表示するには、表示する操作を選択して「**表示**」を選択してから「**スケジュールの詳細**」をクリックします。
 - スケジュール操作の時間を変更するには、変更する操作を選択して「**表示**」を選択してから「**新しい時間範囲**」をクリックします。
 - スケジュール操作をソートするには、「**ソート**」を選択してから表示されるソート・カテゴリーのいずれかをクリックします。
4. HMC ワークスペースに戻るには、「**オプション**」を選択してから「**終了**」をクリックします。
- 操作のスケジュールの詳細については、オンライン・ヘルプを利用してください。

ライセンスの表示

この ハードウェア管理コンソール (HMC) について同意したライセンス内部コードを表示します。

ライセンスは、いつでも表示させることができます。ライセンスを表示するには、次の手順を完了します。

1. ナビゲーション領域で、**HMC 管理アイコン**  をクリックしてから、「**コンソール管理**」を選択します。
2. コンテンツ・ペインで、「**ライセンスの表示**」をクリックします。
3. いずれかのライセンス・リンクをクリックすると詳細が表示されます。

注：このリストには、別の使用許諾契約書のもとで提供されるプログラムおよびコードは含まれません。

4. 「**了解**」をクリックします。

ハードウェア管理コンソールの更新

ハードウェア管理コンソール (HMC) の内部コードの更新方法と、システム 情報およびシステムの作動可能性の表示方法を説明します。

HMC を更新するには、以下のステップを完了します。

1. ナビゲーション領域で、**HMC 管理アイコン**  をクリックしてから、「**コンソール管理**」を選択します。
2. コンテンツ・ペインで、「**ハードウェア管理コンソールの更新 (Update the Hardware Management Console)**」をクリックします。「**HMC 修正サービスのインストール**」ウィザードが開きます。
3. 「**次へ**」をクリックして、更新プロセスを開始します。
4. ウィザードのステップに従って、更新操作を完了します。
5. このタスクを終了したら、「**完了**」をクリックします。

ハードウェア管理コンソールの更新に関する詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

メディアのフォーマット設定

このタスクは、ディスクまたは USB 2.0 フラッシュ・ドライブ・メモリー・キーをフォーマットします。

ディスクットのフォーマットは、ユーザー指定のラベルを提供することによって可能です。

ディスクットまたは USB 2.0 フラッシュ・ドライブ・メモリー・キーをフォーマットするには、以下の手順を完了します。



1. ナビゲーション領域で、**HMC 管理アイコン** をクリックしてから、「**コンソール管理**」を選択します。
2. コンテンツ・ペインで、「**メディアのフォーマット**」をクリックします。
3. 「**メディアのフォーマット**」ウィンドウから、フォーマットするメディアのタイプを選択して「**了解**」をクリックします。
4. メディアが正しく挿入されていることを確認して「**フォーマット**」をクリックします。「**メディアのフォーマット**」進行ウィンドウが表示されます。メディアがフォーマットされると、「**メディアのフォーマットが完了しました**」ウィンドウが表示されます。
5. 「**了解**」をクリックしてから「**閉じる**」をクリックしてタスクを終了します。

このタスクについて詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

管理コンソール・データのバックアップ

これは、ハードウェア管理コンソール (HMC) ハード・ディスクに保存されている、HMC 操作をサポートする上で重要なデータをバックアップ (またはアーカイブ) するタスクです。

HMC データのバックアップは、HMC または論理区画に関連する情報に変更を加えた後に行います。

HMC ハード・ディスクに保管されている HMC データは、ローカル・システム上の DVD-RAM に保管したり、HMC ファイルシステムにマウントされているリモート・システム (例えば NFS) に保管したり、ファイル転送プロトコル (FTP) を使用してリモート・サイトに送信したりすることができます。

HMC を使用して、以下のデータのような重要データをすべてバックアップすることができます：

- ユーザー設定ファイル
- ユーザー情報
- HMC プラットフォーム構成ファイル
- HMC ログ・ファイル
- 修正サービスのインストールによる HMC 更新

注：アーカイブ・データは、製品 CD からの HMC の再インストールの場合にのみ使用します。

重要な HMC データをバックアップするには、以下の手順を実行します。



1. ナビゲーション領域で、**HMC 管理アイコン** をクリックしてから、「**コンソール管理**」を選択します。
2. 「**コンテンツ**」ペインで、「**管理コンソール・データのバックアップ (Backup Management Console Data)**」をクリックします。
3. 「**管理コンソール・データのバックアップ**」ウィンドウから、実行するアーカイブ・オプションを選択します。
4. 「**次へ**」をクリックして、選択したオプションに関連付けられている該当する指示に従います。
5. 「**了解**」をクリックしてバックアップ処理を続けます。

HMC データのバックアップについて詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

注：

- HMC モデル 7063-CR1 では、DVD メディアはサポートされません。

- HMC バージョン 9.1.940 以降を使用している場合、生成されるバックアップ・ファイルに名前を指定できます。バックアップ・ファイルがサーバー上に存在している場合、「**ファイルの置き換え**」を選択して、同じ名前の既存のファイルの内容を置き換えてください。

管理コンソール・データの復元

このタスクを使用して、HMC の重要なバックアップ・データを復元するリモート・リポジトリを選択します。



1. ナビゲーション領域で、**HMC 管理アイコン** をクリックしてから、「**コンソール管理**」を選択します。
2. コンテンツ・ペインで、「**管理コンソール・データの復元**」をクリックします。
3. 「**管理コンソール・データの復元**」ウィンドウから、「**リモートのネットワーク・ファイル・システム (NFS) サーバーから復元 (Restore from a remote Network File System (NFS) server)**」、「**リモートのファイル転送プロトコル (FTP) サーバーから復元 (Restore from a remote File Transfer Protocol (FTP) server)**」、「**リモートのセキュア・シェル・ファイル転送プロトコル (SFTP) サーバーから復元 (Restore from a remote Secure Shell File Transfer Protocol (SFTP) server)**」、「**リモートの取り外し可能メディアから復元 (Restore from a remote removable media)**」のいずれかをクリックします。
4. 「**次へ**」をクリックして続行するか、「**取消**」をクリックして、何も変更しないでタスクを終了します。

この HMC の重要なバックアップ・データの復元について詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

アップグレード・データの保管

このタスクはウィザードを使用して、アップグレード・データを選択したメディアに保管します。このデータは、現在のソフトウェア・レベルの実行中に作成またはカスタマイズされたファイルを含みます。このデータの選択したメディアへの保管は、HMC ソフトウェアのアップグレード前に実行されます。



1. ナビゲーション領域で、**HMC 管理アイコン** をクリックしてから、「**コンソール管理**」を選択します。
2. コンテンツ・ペインで、「**アップグレード・データの保管**」をクリックします。
3. 「**アップグレード・データの保管**」ウィンドウで、ウィザードに従ってデータの保管に必要なステップを実行します。データを保管するメディアのタイプを選択して、「**次へ**」をクリックしてタスク・ウィンドウのステップを続行します。
4. タスクを終了したら、「**完了**」をクリックします。

アップグレード・データの保管について詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

データ複製の管理

このタスクはカスタマイズ・データの複製を可能または不可にします。カスタマイズ・データの複製によって、この HMC と別の HMC 間でカスタマイズ・コンソール・データの取得または送信が可能になります。

以下のタイプのデータを構成できます。

- カスタマー情報データ
 - 管理者情報 (カスタマー名、アドレス、電話番号など)

- システム情報(システムの管理者名、アドレス、電話番号など)
- アカウント情報(カスタマー番号、企業番号、営業所など)
- グループ・データ
 - すべてのユーザー定義グループ定義
- モデム構成データ
 - リモート・サポート用にモデムを構成
- アウトバウンド接続データ
 - ローカル・モデムを RSF に構成
 - インターネット接続を使用可能に設定
 - 外部時間ソースに構成

注: 他の HMC からのカスタマイズ可能コンソール・データは、特定の HMC およびそれに関連して許容できるカスタマイズ可能データ・タイプが構成されている場合のみ、その HMC から受け入れます。

データ複製を管理するには、以下の手順を実行します。



1. ナビゲーション領域で、**HMC 管理アイコン** をクリックしてから、「**コンソール管理**」を選択します。
2. コンテンツ・ペインで、「**データ複製の管理**」をクリックします。
3. 「**データ複製の管理**」ウィンドウから、実行する該当のオプションを選択します。

カスタマイズ可能データの複製を可能または不可にすることについて、詳しくはオンライン・ヘルプを利用してください。

テンプレートおよび OS イメージ

システムのテンプレートにはリソース (システム・プロパティ、共有プロセッサ・プール、予約ストレージ・プール、共用メモリー・プール、ホスト・イーサネット・アダプター、SR-IOV アダプターなど) に関する構成の詳細が含まれています。個別タスクを使用して事前に構成した多数のシステム設定は、「テンプレートからシステムをデプロイ」ウィザードから使用可能です。例えば、ウィザードを使用してシステム・テンプレートからシステムをデプロイする場合、バーチャル I/O サーバー、仮想ネットワーク・ブリッジ、および仮想ストレージ設定を構成できます。

テンプレート・ライブラリーには、定義済みのシステム・テンプレートが収容されており、テンプレートには共通の使用シナリオに基づいた構成設定が含まれています。定義済みのシステム・テンプレートは、すぐに利用することができます。テンプレート・ライブラリーで利用できるテンプレートの表示、変更、デプロイ、コピー、インポート、エクスポート、または削除を行います。

また、ユーザーの環境に特有の構成設定を組み込んだカスタムのシステム・テンプレートを作成することもできます。カスタム・テンプレートを作成するには、定義済みテンプレートをコピーし、ユーザーの要件に合わせて変更します。また、既存のシステム構成を取り込んで、その詳細をテンプレートに保存することができます。その後で、そのテンプレートを同じ構成を必要とする他のシステムにデプロイできます。

テンプレート・ライブラリーにアクセスするには、以下の手順を実行します。



1. ナビゲーション領域で、**HMC 管理アイコン** をクリックしてから、「**テンプレートおよび OS イメージ**」を選択します。
2. 「**テンプレートおよび OS イメージ (Templates and OS Images)**」ウィンドウから、以下にアクセスできます。
 - システム
 - 区画
 - OS および VIOS のイメージ

3. このタスクを完了したら、「閉じる」をクリックします。

システムのテンプレート

システムのテンプレートには、リソース (共用プロセッサ・プール、予約ストレージ・プール、共用メモリー・プール、物理 I/O アダプター、ホスト・イーサネット・アダプター、シングル・ルート I/O 仮想化 (SRIOV) アダプター、仮想 I/O サーバー (VIOS)、仮想ネットワーク、および仮想ストレージなど) に関する構成情報が含まれています。

ご使用の環境に固有の構成設定を含んでいるカスタム・システム・テンプレートを作成することができます。定義済みのテンプレートをコピーし、必要に応じて変更することで、カスタム・テンプレートも作成できます。また、既存のシステム構成を取り込んで、その詳細をテンプレートに保存することができます。その後で、そのテンプレートを同じ構成を必要とする他のシステムにデプロイできます。テンプレート名をクリックすると、そのテンプレートに関する詳細が表示されます。表示、編集、コピー、削除、デプロイ、またはエクスポートの対象とするシステム・テンプレートをリストから選択します。

システム・テンプレートについてさらに情報が必要な場合は、オンライン・ヘルプを使用してください。

区画のテンプレート

区画テンプレートには、物理アダプター、仮想ネットワーク、ストレージ構成などの区画リソースに関する詳細が入っています。

ご使用の環境に固有の構成設定を含んでいるカスタム区画テンプレートを作成することができます。定義済みのテンプレートをコピーし、必要に応じて変更することで、カスタム・テンプレートも作成できます。また、既存のシステム構成を取り込んで、その詳細をテンプレートに保存することができます。その後で、そのテンプレートを同じ構成を必要とする他のシステムにデプロイできます。テンプレート名をクリックすると、そのテンプレートに関する詳細が表示されます。表示、編集、コピー、削除、デプロイ、またはエクスポートの対象とする区画テンプレートをリストから選択します。

注:

- HMC バージョン 9.1.940 以降を使用していて、取り込まれていないテンプレートを使用して論理区画を作成している場合、移行可能な SR-IOV 論理ポートを構成できます。区画テンプレートの「編集」メニューの「移行可能」を選択します。バックアップ・デバイスを作成することで SR-IOV 論理ポートを使用して論理区画を移行し、SR-IOV 論理ポートを論理区画に関連付けることができます。バックアップ・デバイスは、仮想イーサネット・アダプターまたは仮想ネットワーク・インターフェース (NIC) アダプターにすることができます。
- HMC がバージョン 9.1.940.x であり、かつファームウェアがレベル FW940 の場合、Hybrid Network Virtualization 機能の「移行可能」オプションは、テクノロジー・プレビューとしてのみ使用でき、実動でのデプロイメントは意図されていません。ただし、HMC がバージョン 9.1.941.0 以降であり、ファームウェアがレベル FW940.10 以降の場合は、Hybrid Network Virtualization 機能の「移行可能」オプションはサポートされます。

区画テンプレートについてさらに情報が必要な場合は、オンライン・ヘルプを使用してください。

VIOS イメージ

VIOS イメージと、ハードウェア管理コンソール (HMC) がアクセスおよび使用できる、オペレーティング環境のインストール・リソースを定義します。

以下のタスクにアクセスできます。

Virtual I/O Server イメージ・リポジトリの管理

HMC バージョン 7.7 以降では、DVD、保存されたイメージ、または Network Installation Management (NIM) サーバーからバーチャル I/O サーバー (VIOS) イメージを HMC に保管できます。保管した VIOS イメージを VIOS のインストールに使用することができます。VIOS イメージをインストールするには、HMC スーパー管理者 (hmcsuperadmin) である必要があります。

このタスクについて

VIOS イメージ・リポジトリを管理またはインポートするには、以下の手順を実行します。

手順



1. ナビゲーション領域で、**HMC 管理アイコン** をクリックしてから、「**テンプレートおよび OS イメージ**」を選択します。
2. 「**テンプレートおよび OS イメージ**」ウィンドウから、「**OS および VIOS のイメージ (OS and VIOS Images)**」タブを選択してから、「**Virtual I/O Server イメージ・リポジトリの管理**」をクリックします。
3. 「**Virtual I/O Server イメージ・リポジトリ**」ウィンドウで、「**新規バーチャル I/O サーバー・イメージのインポート**」をクリックします。
4. 「**新規バーチャル I/O サーバー・イメージのインポート**」ウィンドウで、DVD またはファイルシステムから VIOS イメージを選択してインポートします。
 - VIOS イメージを DVD から HMC にインポートするには、以下のステップを実行します。
 - a. 「**バーチャル I/O サーバー・イメージのインポート (Import Virtual I/O Server Image)**」ウィンドウで、「**管理コンソール DVD (Management console DVD)**」を選択します。
 - b. 「**名前**」フィールドで、DVD からインポートする VIOS イメージの名前を入力します。
 - c. 「**了解**」をクリックします。
 - VIOS イメージをネットワーク・ファイル・システム (NFS)、ファイル転送プロトコル (FTP)、またはセキュア・シェル・ファイル転送プロトコル (SFTP) からインポートするには、以下のステップを実行します。
 - a. 「**バーチャル I/O サーバー・イメージのインポート**」ウィンドウで、「**ファイルシステム**」を選択します。
 - b. 「**リモート NFS サーバー**」、「**リモート FTP サーバー**」、または「**リモート SFTP サーバー**」を選択します。
 - c. 必要な詳細を入力して、「**了解**」をクリックします。

Virtual I/O Server バックアップの管理

HMC バージョン 9.2.950 以降を使用すると、Virtual I/O Server の I/O 構成を管理でき、管理コンソール上で VIOS イメージのバックアップを管理できます。

このタスクについて

VIOS の I/O 構成のバックアップ操作または復元操作を管理し、VIOS イメージを管理するには、以下の手順を実行します。

手順



1. ナビゲーション領域で、**HMC 管理アイコン** をクリックしてから、「**テンプレートおよび OS イメージ**」を選択します。
2. 「**テンプレートおよび OS イメージ**」ウィンドウで、「**VIOS イメージ**」タブを選択してから「**Virtual I/O Server バックアップの管理**」をクリックします。
3. 「**Virtual I/O Server バックアップの管理**」ウィンドウで、「**Virtual I/O Server 構成のバックアップ (Virtual I/O Server Configuration Backup)**」タブを選択します。HMC が取った VIOS 構成のすべてのバックアップ・ファイルをリストした表が表示されます。さらに、構成ファイルが最後に編集された時刻を表示できます。
 - a) VIOS の入出力構成のバックアップを取るには、「**I/O 構成のバックアップ (Backup I/O configuration)**」をクリックします。「**I/O 構成のバックアップ (Backup I/O configuration)**」ウィンドウで、管理対象システムおよびバックアップを作成する VIOS を選択してから、バックアップ・ファイルの名前を指定します。

指定する名前は、ファイル拡張子 **.tar.gz** も含めて 1 文字から 40 文字までで構成されていなければなりません。使用できる文字は、A から Z までの文字、a から z までの文字、0 から 9 までの数字、ドット文字 (.), ダッシュ文字 (-), および下線文字 (_) です。

- b) HMC 内に保管されている既存のバックアップ・ファイルを名前変更するには、表から構成ファイルを選択し、「**アクション**」 > 「**名前変更**」をクリックします。
 - c) VIOS 入出力構成を復元するには、復元したい VIOS の I/O 構成が入っているバックアップ・ファイルを選択し、「**アクション**」 > 「**復元**」をクリックします。
4. 「Virtual I/O Server バックアップの管理」ウィンドウで、「**Virtual I/O Server バックアップ (Virtual I/O Server Backup)**」タブをクリックします。HMC に取られたすべての VIOS イメージ・バックアップをリストした表が表示されます。さらに、VIOS イメージの名前とサイズ、VIOS イメージ・ファイルが最後に編集された時刻、イメージが取り込まれた管理対象システムと VIOS も表示できます。
- a) VIOS イメージのバックアップを取るには、「**バックアップの作成 (Create Backup)**」をクリックします。「バックアップの作成 (Create Backup)」ウィンドウで、管理対象システムおよびバックアップを作成する VIOS を選択してから、バックアップ・ファイルの名前を指定します。
- 指定する名前は、ファイル拡張子 **.tar** も含めて 1 文字から 40 文字までで構成されていなければなりません。使用できる文字は、A から Z までの文字、a から z までの文字、0 から 9 までの数字、ドット文字 (.), ダッシュ文字 (-), および下線文字 (_) です。
- b) HMC 内に保管されている既存の VIOS イメージ・バックアップ・ファイルを名前変更するには、表からバックアップ・ファイルを選択し、「**アクション**」 > 「**名前変更**」をクリックします。
 - c) HMC から VIOS イメージ・バックアップ・ファイルを除去するには、除去したい VIOS 構成が入っているバックアップ・ファイルを表から選択し、「**アクション**」 > 「**除去**」をクリックします。
5. 「**了解**」をクリックします。

すべてのシステム・プラン

システム・プランは、単一管理対象システムの論理区画構成の仕様です。

テーブルに、管理対象システムの構成に使用できるすべてのシステム・プランがリストされます。独自のシステム・プランを作成するか、既存のシステム・プランをインポートすることができます。

システム・プランの作成

このハードウェア管理コンソール (HMC) が管理するシステムの新規システム・プランを作成できます。この新規システム・プランには、プランの作成に使用した管理対象システムの論理区画およびパーティション・プロファイルの仕様が含まれています。

1. 「**作成**」をクリックします。
2. 選択可能なリストから管理対象システムを選択して、「**システム・プラン名**」フィールドおよび「**プランの説明**」フィールドに記入します。
3. 必要なオプションを確認します。
4. 「**作成**」をクリックします。

システム・プランのインポート

ハードウェア管理コンソール (HMC) に、システム・プラン・ファイルをインポートすることができます。この新規システム・プランには、プランの作成に使用した管理対象システムの論理区画およびパーティション・プロファイルの仕様が含まれています。

1. 「**インポート**」をクリックします。
2. システム・プラン・ファイルを HMC にインポートするためのソースを選択します。
3. 「**インポート**」をクリックします。

システム・プランのエクスポート

ハードウェア管理コンソール (HMC) から、システム・プラン・ファイルにエクスポートすることができます。

1. リストからシステム・プランを選択して、「アクション」 > 「エクスポート」とクリックします。
2. システム・プラン・ファイルを HMC にエクスポートするためのソースを選択します。
3. 「エクスポート」をクリックします。

システム・プランのデプロイ

システム・プラン・ファイルを、HMC が管理する 1 つ以上のシステムにデプロイすることができます。システム・プランをデプロイする管理対象システムのハードウェアは、システム・プラン内のハードウェアと同じものでなければなりません。

1. リストからシステム・プランを選択して、「アクション」 > 「デプロイ」とクリックします。
2. 「システム・プランのデプロイ」ウィザードに示される指示に従います。

システム・プランの削除

ハードウェア管理コンソール (HMC) から、システム・プラン・ファイルを削除することができます。

1. リストからシステム・プランを選択して、「アクション」 > 「削除」とクリックします。

最新表示 (Refresh)

テーブルを最新の情報に更新して、使用可能なシステム・プランに対する最新の変更を確認することができます。

1. 「最新表示」をクリックして、最新のデータでテーブルを更新します。

このタスクについて詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

ユーザーおよびセキュリティのタスク

HMC 上で「ユーザーおよびセキュリティ」タスクに使用可能なタスクについて説明します。

注: ユーザー ID に割り当てられたタスク・ロールに応じて、すべてのタスクにはアクセスできない場合があります。タスクとそれらのタスクにアクセス可能なユーザー・ロールのリストは、[9 ページの『HMC タスク、ユーザー・ロール、ID、および関連コマンド』](#)を参照してください。

ユーザー・パスワードの変更

このタスクは、ハードウェア管理コンソール (HMC) にログオンするために使用した既存のパスワードを変更できるようにします。パスワードによって、コンソールにログインするユーザー ID および権限が検証されます。

パスワードを変更するには、以下の手順を実行します。

1. ナビゲーション領域で、管理対象システムを選択し、「ユーザーおよびセキュリティ」アイコンをクリックしてから、「ユーザーおよびロール」を選択します。
2. コンテンツ・ペインで、「ユーザー・パスワードの変更」をクリックします。
3. 「ユーザー・パスワードの変更」ウィンドウから、現在のパスワードを指定し、使用する新規パスワードを指定し、確認のために表示されたフィールドに新規パスワードを再度指定します。

注: 指定する新規パスワードは、少なくとも 8 文字の長さが必要です。



4.「了解」をクリックして変更を続けます。

パスワードの変更について詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

ユーザー・プロファイルおよびアクセスの管理

HMC にログオンするシステム・ユーザーを管理します。ユーザー・プロファイルは、ユーザー ID、サーバー認証方式、許可、およびテキスト記述の組み合わせです。許可は、ユーザーがアクセス許可を持つオブジェクトに関するユーザー・プロファイルに割り当てられた権限レベルを表します。

ユーザーを認証するには、HMC 上でローカル認証を使用するか、Kerberos リモート認証を使用するか、LDAP 認証を使用できます。HMC 上での Kerberos 認証のセットアップについての詳細は、[96 ページの『KDC の管理』](#)を参照してください。LDAP 認証の詳細については、[95 ページの『LDAP の管理』](#)を参照してください。

セキュリティ上の理由から、リモート側で認証済みの Kerberos ユーザーおよび LDAP ユーザーは、ローカル・コンソールをロックできません。

ローカル認証を使用している場合、ユーザー ID およびパスワードは HMC にログオンする際にユーザーの権限を検証するために使用されます。ユーザー ID は、先頭が英字で、1 から 32 文字の英数字でなければなりません。パスワードには次の規則があります。

- 先頭文字は英数字にします。
- 8 文字以上であることが必要ですが、システム管理者は、この制限を変更できます。
- 文字は、標準 7 ビットの ASCII 文字を使用します。
- パスワードに使用できる有効な文字は、A-Z、a-z、0-9 および特殊文字 (~ ! @ # \$ % ^ & * () _ + - = { } [] ¥ . : " ; ') です。

Kerberos 認証を使用している場合は、Kerberos リモート・ユーザー ID を指定します。

LDAP 認証を選択した場合、詳細情報は不要です。

ユーザー・プロファイルには、ユーザーに割り当てられた管理対象リソース・ロールおよびタスク・ロールが含まれます。管理対象リソース・ロールは、管理対象オブジェクトまたはオブジェクトのグループに対する許可を割り当て、タスク・ロールは管理対象オブジェクトまたはオブジェクトのグループに対して実行するユーザーのアクセス・レベルを定義します。ロールは、使用可能なデフォルト管理対象リソース・ロール、タスク・ロールのリスト、または「[タスクおよびリソース・ロールの管理](#)」タスクによって作成されたカスタマイズ・ロールのリストから選択できます。

すべての HMC タスクおよび各タスクを実行できる事前定義されたデフォルトのユーザー ID のリストについては、[9 ページの『HMC タスク、ユーザー・ロール、ID、および関連コマンド』](#)を参照してください。

次の管理対象リソース・ロールがデフォルトで事前定義されています。

- すべてのシステム・リソース

次のタスク・ロールがデフォルトで事前定義されています。

- hmcshervicerep (サービス担当員)
- hmcviewer (ビューアー)
- hmcoperator (オペレーター)
- hmcpe (製品エンジニア)
- hmcsuperadmin (スーパー管理者)

ユーザー・プロファイルを追加またはカスタマイズするには、以下のステップを実行します。

1. ナビゲーション領域で、管理対象システムを選択し、「ユーザーおよびセキュリティ」アイコンをクリックしてから、「ユーザーおよびロール」を選択します。
2. コンテンツ・ペインで、「ユーザー・プロファイルおよびアクセスの管理」をクリックします。
3. 以下のいずれかの手順を実行します。



- 新しいユーザー ID を作成する場合は、「**ユーザー・プロファイル**」ウィンドウでメニューバーの「**ユーザー**」を選択し、そのメニューが表示されたら「**追加**」をクリックします。「**ユーザーの追加**」ウィンドウが表示されます。
- 既存のプロファイルと同じ属性を使用してユーザー ID を作成する場合、「**ユーザー・プロファイル**」ウィンドウでメニューバーの「**ユーザー**」を選択し、そのメニューが表示されたら、「**コピー**」をクリックします。「**ユーザーのコピー**」ウィンドウが表示されます。

注: デフォルト ID など、一部のユーザー・プロファイルは事前定義済みであり、それらの許可は変更できません。ただし、オペレーターなど、デフォルトのユーザー・プロファイルをコピーしてから、その結果として得られた新規ユーザー・プロファイルを変更することはできます。新たに定義されたユーザーは、コピー元のユーザー・プロファイルよりも大きな許可を持つことはできません。

- 「**ユーザー・プロファイル**」ウィンドウで、ユーザー ID を削除する場合はメニューバーの「**ユーザー**」を選択し、そのメニューが表示されたら「**削除**」をクリックします。「**ユーザーの削除 (Remove User)**」ウィンドウが表示されます。
- ユーザー ID がウィンドウに存在する場合、「**ユーザー・プロファイル**」ウィンドウでリストからそのユーザー ID を選択して、メニューバーの「**ユーザー**」を選択し、そのメニューが表示されたら「**変更**」をクリックします。「**ユーザーの変更**」ウィンドウが表示されます。
 - タイムアウト値および非活動状態値を指定するには、「**ユーザーの変更**」ウィンドウから「**ユーザー属性**」をクリックします。

4. ウィンドウのフィールドについて入力または変更を完了したら「**了解**」をクリックします。

ユーザー・プロファイルの作成、変更、コピー、除去、およびタイムアウト値と非活動状態値について詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

ユーザー・プロファイルの追加、コピー、または変更

ユーザー・プロファイルの追加、コピー、または変更の方法について説明します。

Kerberos または Lightweight Directory Access Protocol (LDAP) を使用してリモートで認証するユーザーは、そのプロファイルがそれぞれ適宜設定されている必要があります。リモートで認証された Kerberos または LDAP の各ユーザーのユーザー・プロファイルを、ローカル認証ではなく、そのタイプの認証を使用するように設定する必要があります。Kerberos または LDAP のリモート認証を使用するよう設定されたユーザーは、HMC にローカルでログインする場合でも、常にそのタイプの認証を使用します。

注: Kerberos 認証を使用するには、「**KDC の構成**」タスクを使用した鍵配布センター (KDC) サーバーの構成が必要です。LDAP 認証を使用するには、「**LDAP 構成**」タスクを使用した LDAP サーバーの構成が必要です。すべてのユーザーを、Kerberos または LDAP のリモート認証を使用するよう設定する必要はありません。一部のユーザーについては、ローカル認証のみを使用できるように、そのユーザー・プロファイルを設定することができます。

「ユーザー・プロファイルの追加、コピー、または変更」ウィンドウで、以下の属性を変更することができます。

- **ユーザー ID:** 作成または管理しているユーザー・プロファイルのユーザー ID を入力します。ユーザー名は、先頭が英字で、1 文字から 32 文字の英数字でなければなりません。
- **説明:** ユーザー独自のレコードについて分かりやすい説明を入力します。
- **パスワード:** ユーザー ID のパスワードを入力します。
- **パスワードの確認:** 確認のためにパスワードを再度入力します。
- **パスワードが期限切れになるまでの日数:** パスワードの有効期限が切れるまでの日数を指定します。この入力フィールドは、「**厳密なパスワード規則の適用 (Enforce strict password rules)**」チェック・ボックスが選択されている場合のみ使用できます。
- **リソース・ロールの管理 (Manage resource roles):** 現在使用可能な管理対象リソース・ロールを表示します。このユーザー ID のアクセス許可を定義するために 1 つ以上の管理対象リソース・ロールを選択してください。
- **タスク・ロール:** 現在使用可能なタスク・ロールを表示します。このユーザー ID のタスク・ロールを 1 つ以上選択してください。

ユーザー・プロファイルの作成、変更、コピー、除去、または削除、およびタイムアウト値と非活動状態値に関する詳細情報が必要な場合は、オンライン・ヘルプを使用してください。

ユーザー属性

特定のユーザーについてのタイムアウト値および非活動状態値を指定する方法について説明します。

以下のタイムアウト・タスクおよび非活動タスクの時間の長さを指定できます。

タイムアウト値

- **セッション・タイムアウト時間 (分):** ユーザーがログオン・セッション中にプロンプトで ID 確認を求められる時間 (分) を指定します。ゼロ以外の値が指定された場合、指定の時間が経過した後で、ユーザーにパスワードの再入力を求めるプロンプトが出されます。「**タイムアウト時間 (分) の検査**」フィールドに指定された時間内にパスワードが再入力されない場合、セッションは切断されます。
- **タイムアウト時間 (分) の検査:** 「**セッション・タイムアウト時間 (分)**」フィールドに値が指定されていた場合に、ユーザーがプロンプトでパスワードの再入力を求められたときに再入力しなければならない時間の長さを指定します。指定された時間内にパスワードが再入力されない場合、セッションは切断されます。
- **アイドル・タイムアウト時間 (分):** ユーザーのセッションがアイドルでいられる時間 (分) を指定します。ユーザーが指定の時間内にセッションと対話しない場合、セッションはロックされ、スクリーンセーバーが開始されます。スクリーンの任意の場所をクリックすると、ユーザーに ID 確認を求めるプロンプトが出されます。
- **パスワード変更間隔の最短期間 (日):** ユーザーのパスワードを変更するのに必要な間隔の最短期間 (日) を指定します。

注: 上記のフィールドのいずれであっても、ゼロの注がある場合は、時間の満期がないことを表します。これがデフォルト値です。最大で 525600 分 (1 年に相当) という最大値を指定することができます。

非活動状態値

- **非活動状態のために使用不可になる (日数):** 非活動の最大日数に達した後でユーザーが一時的に無効になる時間の長さを日単位で指定します。
- **非活動状態のために使用不可にはならない:** 非活動状態のためにユーザーのセッションを使用不可にしないオプション。
- **Web を介したリモート・アクセスを許可:** 管理しているリモート Web サーバー・アクセスをユーザーに対して使用可能にするオプション。

ユーザーとタスクの管理

ログオンしているユーザーおよびそのユーザーが実行しているタスクを表示します。



1. ナビゲーション領域で、管理対象システムを選択し、「**ユーザーおよびセキュリティ**」アイコンをクリックしてから、「**ユーザーおよびロール**」を選択します。
2. コンテンツ・ペインで、「**ユーザーとタスクの管理**」をクリックします。
3. 「ユーザーとタスクの管理」ウィンドウに次の情報が表示されます。
 - ログイン時に使用したユーザー
 - ログインした時刻
 - 実行中のタスクの数
 - アクセス・ロケーション
 - 実行中のタスクの情報:
 - タスク ID
 - タスク名
 - ターゲット (ある場合)

– セッション ID

4. 実行中のセッションからは、ユーザーの「**ログオン**」リストからセッションを選択して、「**ログオフ**」または「**切断**」をクリックすることによって、ログオフまたは切断を選択できます。
または、「**実行中のタスク (Running Tasks)**」リストからタスクを選択して、「**切り替え**」または「**終了**」をクリックして、別のタスクへの切り替え、またタスクの終了を選択できます。
5. このタスクを終了したら、「**閉じる**」をクリックします。

タスク・ロールおよびリソース・ロールの管理

このタスクを使用して、ユーザー・ロールの定義およびカスタマイズを行います。

注: 定義済みのロール (デフォルト・ロール) に変更を加えることはできません。

ユーザー・ロールとは権限を収集したものです。ユーザー・ロールを作成すると、指定したユーザーのクラスに許可されるタスクのセット (タスク・ロール) を定義したり、ユーザーが管理可能な管理対象オブジェクトのセット (管理対象リソース・ロール) を定義できます。ユーザー・ロールを定義またはカスタマイズしておくと、「**ユーザー・プロファイルおよびアクセスの管理 (Manage User Profiles and Access)**」タスクを使用して、新しいユーザーをそれ自身の許可を指定して作成できます

コマンド行インターフェースまたは REST API CLI 実行プログラムのジョブのいずれかを使用してハードウェア管理コンソール (HMC) でリソース・ロールの自動更新機能が有効になっている場合、HMC ユーザーは、作成された論理区画に対する許可を自動的に受け取ることができます。論理区画が削除されると、許可は自動的に取り消されます。

次の管理対象リソース・ロールが事前定義されています。

- すべてのシステム・リソース

次のタスク・ロールが事前定義されています。

- hmcshervicerep (サービス担当員)
- hmcviewer (ビューアー)
- hmcoperator (オペレーター)
- hmcpe (製品エンジニア)
- hmcsuperadmin (スーパー管理者)

管理対象リソース・ロールまたはタスク・ロールをカスタマイズする場合:

1. ナビゲーション領域で、管理対象システムを選択し、「**ユーザーおよびセキュリティ**」アイコンをクリックしてから、「**ユーザーおよびロール**」を選択します。
2. コンテンツ・ペインで、「**タスク・ロールおよびリソース・ロールの管理**」をクリックします。
3. 「**タスクおよびリソース・ロールの管理**」ウィンドウで「**管理対象リソース・ロール**」または「**タスク・ロール**」のいずれかを選択します。
4. ロールを追加する場合は、メニューバーの「**編集**」をクリックして「**追加**」をクリックし、新しいロールを作成します。

または

既存のロールをコピー、除去、または変更する場合は、カスタマイズするオブジェクトを選択して、メニューバーの「**編集**」をクリックし、「**コピー**」、「**除去**」、または「**変更**」をクリックします。

5. タスクを終了したら、「**終了**」をクリックします。

管理対象リソース・ロールおよびタスク・ロールのカスタマイズの詳細については、オンライン・ヘルプを利用してください。



証明書管理

このタスクを使用して、ご使用の HMC で使用する証明書を管理します。このタスクによって、コンソールで使用する証明書に関する情報を取得できます。またこのタスクによって、コンソールに対して新しい証明書の作成、証明書のプロパティ値の変更、および既存またはアーカイブされている証明書または署名する証明書を処理することができます。

HMC へのすべてのリモート・ブラウザー・アクセスでは、Secure Sockets Layer (SSL) 暗号化を使用する必要があります。HMC へのすべてのリモート・アクセスに SSL 暗号化が必要なことから、証明書はこの暗号化に対するキーを提供する必要があります。HMC はこの暗号化が行われる自己署名証明書を提供します。

証明書を管理する場合:



1. ナビゲーション領域で、管理対象システムを選択し、「ユーザーおよびセキュリティ」アイコンをクリックしてから、「ユーザーおよびロール」を選択します。
2. コンテンツ・ペインで、「証明書の管理」をクリックします。
3. 証明書とともに実行する処理については、以下のように「証明書管理」ウィンドウのメニューバーを使用します。
 - コンソールの新しい証明書を作成する場合は、「作成」をクリックしてから「新規証明書 (New Certificate)」を選択します。証明書が自己署名か、認証局 (CA) の署名か決定して「了解」をクリックします。
 - 自己署名証明書のプロパティ値を変更する場合は、「選択済み」をクリックして「変更」を選択します。必要な変更を加えて「了解」をクリックします。

注: 認証局 (CA) によって署名された証明書があり、その証明書がルート証明書、中間証明書、およびクライアント証明書またはリーフ証明書から構成されている場合は、以下の手順を実行して、証明書を HMC にアップロードします。

- テキスト・ベースのエディターを使用して CA 署名証明書ファイルを開き、ファイルのコンテンツを分割して 3 つの個別ファイルとして保管します。1 つ目のファイルはクライアント証明書またはリーフ証明書、2 つ目のファイルは中間証明書、3 つ目のファイルはルート証明書です。
 - HMC にログインして証明書をインポートします。最初にクライアント証明書をアップロードし、「はい」をクリックして他のファイルをアップロードします。新規ウィンドウで、中間証明書およびルート証明書をアップロードします。
 - 「了解」をクリックしてコンソールを再始動します。
 - 既存またはアーカイブされた証明書、または署名する証明書を処理する場合は、「拡張機能」をクリックします。ここで以下のオプションを選択できます。
 - 既存の証明書の削除 (Delete existing certificates)
 - アーカイブ済み証明書の処理 (Work with archived certificates)
 - 証明書のインポート (Import certificates)
 - 発行者証明書の表示 (View issuer certificates)
4. 「適用」をクリックして、すべての変更を有効にします。

証明書の管理について詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

証明書失効リストの管理

このタスクを使用して、ハードウェア管理コンソール (HMC) 上で使用される証明書失効リストの作成、変更、削除、およびインポートを行うことができます。

HMC にアクセスするすべてのリモート・ブラウザでは、Secure Sockets Layer (SSL) 暗号化を使用する必要があります。この暗号化のための鍵を提供するためには、証明書が必要です。HMC はこの暗号化が行われる自己署名証明書を提供します。

証明書失効リストを管理するには、次の手順を完了します。



1. ナビゲーション領域で、管理対象システムを選択し、「ユーザーおよびセキュリティー」アイコンをクリックしてから、「ユーザーおよびロール」を選択します。
 2. コンテンツ・ペインで、「証明書失効リストの管理」をクリックします。
 3. 証明書とともに実行する処理については、以下のように「証明書失効リストの管理」ウィンドウのメニューバーを使用します。
 - ・ コンソールの新しい証明書失効リストを作成する場合は、「インポート」をクリックしてから「新規証明書失効リスト (New CRL)」を選択します。証明書失効リストを、コンソールの取り外し可能メディアからインポートするのか、あるいは Web ブラウザーを実行中のシステムのファイルシステムから、インポートするのかを決定します。
- 注：リストが取り外し可能メディアからのものである場合、証明書失効リスト・ファイルがメディアのトップ・ディレクトリー内になければなりません。
- ・ コンソール上で証明書失効リストを変更する場合は、テーブルから目的の証明書失効リストを選択し、適切な変更を行ってから「適用」をクリックします。
 - ・ コンソールから証明書失効リストを削除する場合は、「選択済み」をクリックしてから、「証明書失効リストの削除 (Delete CRL)」を選択します。目的の証明書失効リストを選択してから、「OK」をクリックします。
 - ・ 既存またはアーカイブされた証明書、または署名する証明書を処理する場合は、「拡張機能」をクリックします。

証明書失効リストの管理について詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

LDAP の管理

LDAP (Lightweight Directory Access Protocol) 認証が使用されるように、ご使用の HMC を構成します。

始める前に

注：LDAP 認証が使用されるように HMC を構成する前に、HMC と LDAP サーバーの間に機能しているネットワーク接続があることを確認する必要があります。

このタスクについて

LDAP 認証が使用されるように HMC を構成するには、次を実行してください。

手順



1. ナビゲーション領域で、管理対象システムを選択し、「ユーザーおよびセキュリティー」アイコンをクリックしてから、「システムおよびコンソール・セキュリティー」を選択します。
2. コンテンツ・ペインで、「LDAP の管理」をクリックします。「LDAP サーバー定義」ウィンドウが開きます。
3. 「LDAP を使用可能にする (Enable LDAP)」を選択します。
4. 認証に使用するために、LDAP サーバーを定義します (例えば、Microsoft Active Directory、Tivoli®、および Open LDAP)。
5. 認証済みユーザーの識別に使用される LDAP 属性を定義します。デフォルトは **uid** ですが、独自の属性を使用することができます。Microsoft Active Directory の場合は、属性として「**sAMAccountName**」を使用します。

6. 識別名のツリー (検索ベースとも呼ばれる) を LDAP サーバーに対して定義します。

7. 「了解」をクリックします。

次のタスク

LDAP 認証を使用する場合は、ローカル認証ではなく LDAP リモート認証が使用されるように各リモート・ユーザーのプロファイルを構成する必要があります。

KDC の管理

このハードウェア管理コンソール (HMC) によって Kerberos リモート認証に使用される鍵配布センター (KDC) サーバーを表示します。

このタスクから、次のタスクを完了します。

- 既存の KDC サーバーを表示する。
- レルム、チケット存続時間、クロック・スキューなどの、既存の KDC サーバー・パラメーターを変更する。
- HMC 上で KDC サーバーを追加および構成する。
- KDC サーバーを除去する。
- サービス・キーをインポートする。
- サービス・キーを除去する。

Kerberos は、共通鍵の暗号方式を使用してクライアント/サーバー・アプリケーションで強力な認証を行うように設計されたネットワーク認証プロトコルです。

Kerberos では、クライアント (一般にユーザーまたはサービス) は KDC に対してチケットを求める要求を送信します。KDC はクライアント用にチケット許可チケット (TGT) を作成し、そのクライアントのパスワードを鍵として使用してそのチケットを暗号化した後、暗号化された TGT をクライアントに戻します。クライアントは自身のパスワードを使用して、受け取った TGT の暗号化解除を試みます。クライアントは TGT の暗号化解除に成功すると (例えば、クライアントが正しいパスワードを入力すると)、暗号化解除された TGT をそのまま保持し、その TGT がクライアントの身元証明を示します。

チケットには時刻使用可能期間が設定されています。Kerberos には関与するホスト同士を同期するためのクロックが必要です。HMC クロックが KDC サーバーのクロックと同期されない場合、認証は失敗します。

Kerberos レルムとは、Kerberos リモート認証を使用する管理ドメイン、サイト、または論理ネットワークです。各レルムでは、そのレルムのユーザーとサービスに関する情報を含む、KDC サーバー上に保管されているマスター Kerberos データベースが使用されます。レルムにはさらに 1 つ以上のスレーブ KDC サーバーがある場合もあります。これらのサーバーには、そのレルムのマスター Kerberos データベースの読み取り専用コピーが保管されています。

KDC のスプーフィングを防止するため、KDC に対する認証を行うためのサービス・キーを使用するよう HMC を構成することができます。サービス・キー・ファイルは、キー・タブとも呼ばれます。Kerberos では、要求された TGT が HMC のサービス・キー・ファイルを発行した KDC と同じ KDC によって発行されたことが検証されます。サービス・キー・ファイルを HMC にインポートするには、事前に HMC クライアントのホスト・プリンシパル用のサービス・キーを生成しておく必要があります。

注: MIT Kerberos V5 *nix ディストリビューションでは、KDC で `kadmin` ユーティリティーを実行し、`ktadd` コマンドを使用してサービス・キー・ファイルを作成します。その他の Kerberos のインプリメンテーションでは、異なるプロセスでサービス・キーを作成する必要があります。

サービス・キー・ファイルは以下のいずれかのソースからインポートすることができます。

- オプティカル・ディスクまたは USB 大容量ストレージ・デバイスなど、HMC にマウントされている取り外し可能メディア。このオプションは HMC でローカルに (リモート側ではなく) 使用する必要があり、このオプションの使用前に取り外し可能メディアを HMC にマウントしておく必要があります。
- セキュア FTP を使用するリモート・サイト。SSH がインストールされて実行中の任意のリモート・サイトからサービス・キー・ファイルをインポートできます。

この HMC で Kerberos リモート認証を使用するには、以下の作業を行う必要があります。

- HMC 上で Network Time Protocol (NTP) サービスを有効にして、その同じ NTP サーバーと時刻が同期するように HMC と KDC サーバーを設定する必要があります。HMC 上で NTP サービスを有効にするには、



HMC 管理アイコン から [79 ページの『日付と時刻の変更』](#) タスクにアクセスし、「**コンソール設定**」を選択します。

- ローカル認証ではなく Kerberos リモート認証を使用するよう、各リモート・ユーザーのユーザー・プロファイルを設定する必要があります。Kerberos リモート認証を使用するように設定されたユーザーは、そのユーザーが HMC にローカルでログオンしている場合でも、常に Kerberos リモート認証を使用します。

注: すべてのユーザーを Kerberos リモート認証を使用するように設定する必要はありません。一部のユーザーについては、ローカル認証のみを使用できるように、そのユーザー・プロファイルを設定することができます。

- サービス・キー・ファイルの使用はオプションです。サービス・キー・ファイルを使用する前に、そのファイルを HMC にインポートする必要があります。サービス・キーが HMC にインストール済みの場合は、レルム名がネットワーク・ドメイン名と同じでなければなりません。以下の例は、HMC ホスト名が hmc1、DNS ドメインが example.com、Kerberos レルム名が EXAMPLE.COM であると想定して、**kadmin.local** コマンドを使用して Kerberos サーバー上にサービス・キー・ファイルを作成する方法を示しています。

```
- # kadmin_local kadmin.local: ktadd -k /etc/krb5.keytab host/  
hmc1.example.com@EXAMPLE.COM
```

Kerberos サーバーで Kerberos ktutil を使用して、サービス・キー・ファイルの内容を確認します。出力は、次の例のようになります。

```
- # ktutil  
  
ktutil: rkt /etc/krb5.keytab  
ktutil: l  
  
slot KVN0 Principal  
-----  
-----  
  
1 9 host/hmc1.example.com@EXAMPLE.COM  
2 9 host/hmc1.example.com@EXAMPLE.COM
```

- HMC Kerberos 構成は、GSSAPI を使用するパスワードなしの SSH (セキュア・シェル) ログイン用に変更することができます。Kerberos を介する HMC へのパスワードを使用しないリモート・ログインでは、サービス・キーを使用するように HMC を構成します。この構成が完了したら、**kinit -f principal** を使用してリモート Kerberos クライアント・マシン上で転送可能な信任状を入手します。これで、次のコマンドを実行して HMC にログインします。パスワードを入力する必要はありません。**\$ ssh -o PreferredAuthentications=gssapi-with-mic user@host**

KDC を管理するには、以下の手順を実行します。



1. ナビゲーション領域で、管理対象システムを選択し、「**ユーザーおよびセキュリティ**」アイコンをクリックしてから、「**ユーザーおよびロール**」を選択します。
2. コンテンツ・ペインで、「**KDC の管理**」をクリックします。
3. 「**KDC の管理**」ウィンドウで、「**アクション**」メニューにある選択可能なオプションから該当のタスクを選択します。
4. タスクが完了したら、「**了解**」をクリックします。

KDC の管理について詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

KDC サーバーの表示

ハードウェア管理コンソール (HMC) で既存の鍵配布センター (KDC) サーバーを表示します。

HMC で既存の KDC サーバーを表示するには、**ユーザーおよびセキュリティ** アイコン  をクリックしてから、「**ユーザーおよびロール**」を選択します。コンテンツ・ペインで、「**KDC の構成**」をクリックします。サーバーが存在せず、NTP がまだ有効になっていない場合は、警告パネル・メッセージが表示されます。HMC 上で NTP サービスを有効にして、必要に応じて新しい KDC サーバーを構成します。

KDC サーバーの変更

ハードウェア管理コンソール (HMC) で鍵配布センター (KDC) を変更する方法について説明します。

既存の鍵配布センター (KDC) サーバー・パラメーターを変更するには、以下の手順を実行します。

1. ナビゲーション領域で、管理対象システムを選択し、「**ユーザーおよびセキュリティ**」アイコン  をクリックしてから、「**ユーザーおよびロール**」を選択します。
2. コンテンツ・ペインで、「**KDC の管理**」をクリックします。
3. KDC サーバーを選択します。
4. 変更する値を以下から選択します。
 - **レルム (Realm)**。レルムとは、認証管理可能ドメインです。通常、レルムは常に大文字で表示されます。DNS ドメインと同じレルム名 (大文字) を作成することをお勧めします。ユーザーがレルムに属している状態とは、ユーザーがそのレルムの認証サーバーとキーを共有している場合のみを指します。サービス・キー・ファイルが HMC にインストールされている場合、レルム名はネットワーク・ドメイン名と同じでなければなりません。
 - **チケット 存続時間 (Ticket Lifetime)**。チケット 存続時間は、信任状の存続時間を設定します。このフォーマットは整数の後に、**s** 秒、**m** 分、**h** 時間、または **d** 日のいずれかが続いたものです。Kerberos 存続時間ストリングは *2d4h10m* などと入力します。
 - **Clock skew (クロック・スキュー)**。クロック・スキューは、Kerberos がメッセージを無効とみなすまでの、HMC と KDC サーバーの間におけるクロック・スキューの最大許容時間を設定します。このフォーマットは秒数を表す整数です。
5. 「**了解**」をクリックします。

KDC サーバーの追加

鍵配布センター (KDC) サーバーを、このハードウェア管理コンソール (HMC) に追加します。

新規 KDC サーバーを追加するには、以下の手順を実行します。

1. ナビゲーション領域で、管理対象システムを選択し、「**ユーザーおよびセキュリティ**」アイコン  をクリックしてから、「**ユーザーおよびロール**」を選択します。
2. コンテンツ・ペインで、「**KDC の管理**」をクリックします。
3. 「**アクション**」ドロップダウン・リストから、「**KDC サーバーの追加 (Add KDC Server)**」を選択します。
4. KDC サーバーのホスト名または IP アドレスを入力します。
5. KDC サーバー・レルムを入力します。
6. 「**了解**」をクリックします。

KDC サーバーの除去

ハードウェア管理コンソール (HMC) 上の Kerberos 認証は、すべての鍵配布センター (KDC) サーバーが除去されるまで、使用可能なままに残ります。

KDC サーバーを除去する場合:



1. ナビゲーション領域で、管理対象システムを選択し、「ユーザーおよびセキュリティ」アイコンをクリックしてから、「ユーザーおよびロール」を選択します。
2. コンテンツ・ペインで、「**KDC の管理**」をクリックします。
3. リストから KDC サーバーを選択します。
4. 「アクション」ドロップダウン・リストから、「**KDC サーバーの除去 (Remove KDC Server)**」を選択します。
5. 「了解」をクリックします。

サービス・キーのインポート

サービス・キー・ファイルをハードウェア管理コンソール (HMC) にインポートするには、まずサービス・キー・ファイルを HMC ホストの Kerberos サーバー上に前もって作成しておく必要があります。サービス・キー・ファイルには、HMC クライアントのホスト・プリンシパル (host/example.com@EXAMPLE.COM など) が含まれています。ホスト・サービス・キー・ファイルは、KDC 認証で使用する他に、GSSAPI を使用するパスワードなしの SSH (セキュア・シェル) ログインを使用可能にする場合にも使用します。

注: MIT Kerberos V5 *nix ディストリビューションでは、KDC で `kadmin` ユーティリティを実行し、`ktadd` コマンドを使用してサービス・キー・ファイルを作成します。その他の Kerberos のインプリメンテーションでは、異なるプロセスでサービス・キーを作成する必要があります。

サービス・キーをインポートするには、以下の手順を実行します。



1. ナビゲーション領域で、管理対象システムを選択し、「ユーザーおよびセキュリティ」アイコンをクリックしてから、「ユーザーおよびロール」を選択します。
2. コンテンツ・ペインで、「**KDC の管理**」をクリックします。
3. 「アクション」ドロップダウン・リストから、「**サービス・キーのインポート (Import Service Key)**」を選択します。
4. 以下のいずれかを選択します。
 - ・ **ローカル** - サービス・キーは、現在 HMC 上にマウントされている取り外し可能メディア上になければなりません。このオプションは HMC でローカルに (リモート側ではなく) 使用する必要があり、このオプションの使用前に取り外し可能メディアを HMC にマウントしておく必要があります。メディア上におけるサービス・キー・ファイルの絶対パスを指定してください。
 - ・ **リモート** - サービス・キーは、セキュア FTP を通じて HMC が使用できるリモート・サイト上になければなりません。SSH (セキュア・シェル) がインストールおよび実行されている任意のリモート・サイトからサービス・キー・ファイルをインポートすることができます。そのリモート・サイトのホスト名、ユーザー ID とパスワード、およびそのサイト上におけるサービス・キー・ファイルの絶対パスを指定してください。
5. 「了解」をクリックします。

サービス・キー・ファイルのインプリメンテーションは、HMC がリブートされるまで有効になりません。

サービス・キーの除去

ハードウェア管理コンソール (HMC) からサービス・キーを除去する方法について説明します。

HMC からサービス・キーを除去するには、以下の手順を実行します。



1. ナビゲーション領域で、管理対象システムを選択し、「ユーザーおよびセキュリティ」アイコンをクリックしてから、「ユーザーおよびロール」を選択します。
2. コンテンツ・ペインで、「KDC の管理」をクリックします。
3. 「アクション」ドロップダウン・リストから、「サービス・キーの除去 (Remove Service Key)」を選択します。
4. 「了解」をクリックします。

サービス・キーを除去した後は、HMC をリブートする必要があります。リブートを行わないと、ログイン・エラーの原因となります。

MFA の管理

ハードウェア管理コンソール (HMC) で多要素認証 (MFA) を有効にする方法について説明します。

注：

1. デフォルトでは、HMC での多要素認証は無効にされています。
2. MFA が有効にされており、ユーザーが PowerSC MFA サーバー上で構成されている場合、HMC GUI にログインするには、パスワード・フィールドにキャッシュ・トークン資格情報 (CTC) を入力します。
3. セキュア・シェル (SSH) にログインする場合は、以下のようになります。

MFA が有効にされている場合は、SSH を介してログインするすべてのユーザーに対して、CTC コードの入力を求めるプロンプトが表示されます。ユーザーが PowerSC MFA サーバー上で構成されている場合は、プロンプトに CTC コードを入力することができます。ユーザーが PowerSC MFA サーバー上で構成されていない場合は、CTC コードを求めるプロンプトが表示されたら Enter キーを押して、ユーザーのパスワードをプロンプトに入力します。

多要素認証を有効にするには、以下のステップを実行します。



1. ナビゲーション領域で、「ユーザーおよびセキュリティ」アイコンをクリックし、「システムおよびコンソール・セキュリティ」を選択します。
2. コンテンツ・ペインで、「MFA の管理 (Manage MFA)」をクリックします。
3. 「MFA の管理 (Manage MFA)」ウィンドウから、「多要素認証の有効化 (Enable multi factor authentication)」チェック・ボックスを選択します。
4. 以下の情報を入力します。
 - ・ 認証サーバーのホスト名または IP アドレス
 - ・ 認証サーバーのポート
5. 「了解」をクリックします。

このタスクについて詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

リモート・コマンド実行を有効にする

このタスクは、ssh 機能を使用してリモート・コマンドの実行を可能にするために使用します。



1. ナビゲーション領域で、管理対象システムを選択し、「ユーザーおよびセキュリティ」アイコンをクリックしてから、「ユーザーおよびロール」を選択します。
2. コンテンツ・ペインで、「リモート・コマンド実行を有効にする」をクリックします。
3. 「リモート・コマンド実行を有効にする」ウィンドウから、「ssh 機能を使用してリモート・コマンドを実行可能にする」を選択します。

4.「了解」をクリックします。

リモート操作を有効にする

このタスクは、リモート・ワークステーションから HMC に Web ブラウザーを介してアクセスできるようにするために使用します。

HMC リモート・アクセスを使用可能にするには、以下のようにします。

1. ナビゲーション領域で、管理対象システムを選択し、「ユーザーおよびセキュリティ」アイコン  をクリックしてから、「ユーザーおよびロール」を選択します。
2. コンテンツ・ペインで、「リモート操作を有効にする」をクリックします。
3. 「リモート操作」ドロップダウン・リストから「使用可能」を選択して、「了解」をクリックします。リモート・ワークステーションから、Web ブラウザーを使用して HMC にアクセスすることができます。

HMC へのリモート・アクセスの許可について詳細な情報を取得するには、オンライン・ヘルプを使用してください。

リモート仮想端末を使用可能にする

リモート仮想端末接続とは、論理区画に他のリモート HMC から端末接続することです。このタスクを使用して、リモート・クライアントのリモート仮想端末アクセスを可能にします。

1. ナビゲーション領域で、管理対象システムを選択し、「ユーザーおよびセキュリティ」アイコン  をクリックしてから、「ユーザーおよびロール」を選択します。
2. コンテンツ・ペインで、「リモート仮想端末を使用可能にする」をクリックします。
3. 「リモート仮想端末を使用可能にする」ウィンドウで「リモート仮想端末接続を使用可能にする」を選択してこのタスクを使用可能にします。
4. 「了解」をクリックして変更を活動化します。

リモート端末接続を可能にすることについて、詳しくはオンライン・ヘルプを利用してください。

保守容易性タスク

HMC で保守容易性タスクに使用可能なタスクについて説明します。

注: ユーザー ID に割り当てられたタスク・ロールに応じて、すべてのタスクにはアクセスできない場合があります。タスクとそれらのタスクにアクセス可能なユーザー・ロールのリストは、[9 ページの『HMC タスク、ユーザー・ロール、ID、および関連コマンド』](#)を参照してください。

タスク・ログ

ハードウェア管理コンソール (HMC) 上で現在実行中、または完了したすべてのタスクを表示します。

タスク・ログを表示するには、以下のステップを実行します。

1. ナビゲーション領域で、「保守容易性」アイコン  をクリックしてから、「タスク・ログ」を選択します。
2. タスク・ログに以下のタブが表示されます。

- **タスク名:** タスクの名前を表示します。
- **状況:** タスクの現在の状況 (実行中または完了) を表示します。
- **リソース:** リソースの名前を表示します。
- **リソース・タイプ:** リソースのタイプを表示します。
- **イニシエーター:** タスクを開始したユーザーの名前を表示します。
- **開始時刻:** タスクが開始された時刻を表示します。
- **所要時間:** タスクが完了するのに要した時間の長さを表示します。

タスク・ログの表示について詳しくは、オンライン・ヘルプを使用してください。

コンソール・イベント・ログ

ハードウェア管理コンソール (HMC) 上で発生したシステム・イベントの記録を表示します。システム・イベントとは、プロセスが発生、開始と終了、成功または失敗したことを示す個々のアクティビティです。コンソール・イベント・ログを表示するには、以下の手順を実行します。



1. ナビゲーション領域で、**保守容易性アイコン** をクリックしてから、「**コンソール・イベント・ログ**」を選択します。
2. メニューバーを使用して、別の時刻範囲に変更したり、イベントを要約表示する方法を変更します。表を方法を変えて表示する場合は、表アイコンまたはテーブル・ツールバーの「**アクションの選択 (Select Action)**」メニューも使用できます。
3. イベントの表示を終了したら、メニューバーの「**表示**」を選択し、次に「**終了**」をクリックします。

HMC イベントの表示について、詳しくはオンライン・ヘルプを参照してください。

サービス可能イベント・マネージャー

このタスクは、表示するサービス可能イベントの組み合わせの基準を選択します。基準の選択が終了すると、指定した基準に一致するサービス可能イベントを表示できます。

表示するサービス可能イベントの基準を設定するには、以下の手順を実行します。



1. ナビゲーション領域で、**保守容易性アイコン** をクリックしてから、「**サービス可能イベント・マネージャー**」を選択します。
2. 「**サービス可能イベント・マネージャー**」ウィンドウから、イベント基準、エラー基準、および FRU 基準を指定します。
3. 表示するサービス可能イベントの基準を指定したら「**了解**」をクリックします。

イベントの管理について詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

コール・ホーム機能用イベント・マネージャー (Events Manager for Call Home)

HMC から IBM に送信されるあらゆるデータをモニターおよび承認する方法について説明します。



1. ナビゲーション領域で、**保守容易性アイコン** をクリックしてから、「**コール・ホーム用イベント・マネージャー**」を選択します。
2. 「**コール・ホーム用イベント・マネージャー**」ウィンドウから、登録済みの管理コンソールのリストを管理するために「**コンソールの管理**」を選択します。「**イベント基準**」を使用して、すべての登録済み管理コンソールで利用できるイベントのリストをフィルターに掛けるための承認状態、状況、および発

信元 HMC を指定することができます。基準を使用して表示をフィルターに掛け、イベントを選択して詳細の表示、ファイルの表示、およびコール・ホーム操作の実行を行うことができます。

3. 「了解」をクリックして「コール・ホーム機能用イベント・マネージャー (Events Manager for Call Home)」を終了し、フィルター値を保存します。

このタスクについて詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

サービス可能イベントの作成

このタスクは、ハードウェア管理コンソール (HMC) 上で発生した問題 (例えばマウスが動作しない) をサービス・プロバイダーに報告するか、問題の報告についてのテストを行います。

問題のサブミットは、このハードウェア管理コンソールがリモート・サポート機能 (RSF) を使用するようにカスタマイズされ、サービスを自動的に呼び出すことが許可されているかどうかによって変わります。上記の場合、問題情報とサービス要求はモデム送信によりサービス・プロバイダーに自動的に送信されます。

ご使用のハードウェア管理コンソールに関する問題を報告する場合は、以下の手順を実行します。



1. ナビゲーション領域で、保守容易性アイコン  をクリックしてから、「サービス管理」を選択します。
2. コンテンツ・ペインで、「サービス可能イベントの作成」をクリックします。
3. 「サービス可能イベントの作成」ウィンドウに表示されるリストから問題のタイプを選択します。
4. 「問題記述」入力フィールドに問題の簡単な説明を入力して「サービスの要求」をクリックします。

「問題の報告」ウィンドウで問題の報告をテストする場合:

1. 「自動問題レポート機能のテスト」を選択して、「問題記述」入力フィールドに「単なるテストです (This is just a test)」と入力します。
2. 「サービスの要求」をクリックします。問題はハードウェア管理コンソールのサービス・プロバイダーに報告されます。問題を報告すると、「問題の報告」ウィンドウに入力した情報と、コンソールを識別するマシン情報がサービス・プロバイダーに送信されます。

問題の報告または問題の報告の動作テストについて詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

ダンプの管理

ハードウェア管理コンソール (HMC) で、選択したシステムのダンプの手順を管理する方法について説明します。

ダンプを管理するには、以下の手順を実行します。



1. ナビゲーション領域で、保守容易性アイコン  をクリックしてから、「サービス管理」を選択します。
2. コンテンツ・ペインで、「ダンプの管理」をクリックします。
3. 「ダンプの管理」ウィンドウでダンプを選択し、ダンプに関連する以下のタスクのいずれかを実行します。

メニューバーの「選択済み」から:

- ダンプをメディアにコピーします。
- ダンプをリモート・システムにコピーします。
- コール・ホーム機能を使用して、ダンプをサービス・プロバイダーに伝送します。

- ダンプを削除します。

メニューバーの「アクション」から:

- 管理対象システムのハードウェアおよびサーバー・ファームウェアのダンプを開始します。
- サービス・プロセッサのダンプを開始します。
- 「大容量電源制御」サービス・プロセッサのダンプを開始します。
- ダンプ・タイプのダンプ機能パラメーターを変更します。

メニューバーの「状況」にダンプのオフロード進行度が表示されます。

4. このタスクを終了したら、「了解」をクリックします。

ダンプ管理の詳細については、オンライン・ヘルプを利用してください。

サービス情報の送信

サービス情報をサービス・プロバイダーに即時に送信するか、またはサービス情報を問題判別に使用できるように送信する時期をスケジュールします。

サービス情報をスケジュールまたは送信するには、以下の手順を実行します。



1. ナビゲーション領域で、**保守容易性アイコン** をクリックしてから、「サービス管理」を選択します。
2. コンテンツ・ペインで、「サービス情報の送信」をクリックします。
3. コンテンツ・ペインで、「データのスケジュールおよび送信」タブをクリックしてサービス情報をスケジュールします。

注: 以下のタブをクリックして、送信したいデータの選択および FTP 接続の構成を行うこともできます。

- **データのスケジュールおよび送信:** 情報をサービス・プロバイダーに即時に送信するか、またはその送信をスケジュールします。
 - **FTP 接続の構成:** FTP を使用したサービス情報のオフロードを可能にするための構成データを指定します。
 - **問題レポートの送信:** 必要なデータ、およびそのデータの宛先を選択します。
4. 定期的送信を有効化したいか、または即時に送信したいサービス情報のタイプを選択します。
 - **操作テスト (ハートビート) 情報 -- 常時有効:** 問題イベント・ログ・ファイルを送信します。
 - **ハードウェア・サービス情報 (VPD):** この HMC に接続されているすべての管理対象システムの重要プロダクト・データ (VPD) を送信します。
 - **ソフトウェア・サービス情報:** 各区画で実行されているすべてのソフトウェアの VPD を送信します。
 - **パフォーマンス管理情報:** パフォーマンス管理情報を収集し、送信します。
 - **更新アクセス・キー情報:** アクセス・キー情報を検証し、更新します。
 5. 反復送信をスケジュールするために、間隔 (日単位) と時刻を選択します。情報を即時に送信するためには、「即時送信」をクリックします。
 6. 「了解」をクリックします。

サービス情報のスケジュールについて、詳しくはオンライン・ヘルプを参照してください。

メディアのフォーマット設定

このタスクは、ディスケットまたは USB 2.0 フラッシュ・ドライブ・メモリー・キーをフォーマットします。

ディスケットのフォーマットは、ユーザー指定のラベルを提供することによって可能です。

ディスクまたは USB 2.0 フラッシュ・ドライブ・メモリー・キーをフォーマットするには、以下の手順を完了します。



1. ナビゲーション領域で、**HMC 管理**アイコンをクリックしてから、「**コンソール管理**」を選択します。
2. コンテンツ・ペインで、「**メディアのフォーマット**」をクリックします。
3. 「**メディアのフォーマット**」ウィンドウから、フォーマットするメディアのタイプを選択して「**了解**」をクリックします。
4. メディアが正しく挿入されていることを確認して「**フォーマット**」をクリックします。「**メディアのフォーマット**」進行ウィンドウが表示されます。メディアがフォーマットされると、「**メディアのフォーマットが完了しました**」ウィンドウが表示されます。
5. 「**了解**」をクリックしてから「**閉じる**」をクリックしてタスクを終了します。

このタスクについて詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

Electronic Service Agent セットアップ・ウィザード

ハードウェア管理コンソール (HMC) インターフェースを使用して Electronic Service Agent セットアップ・ウィザードを開く方法について説明します。

このタスクについて

Electronic Service Agent セットアップ・ウィザードを開くには、以下の手順を実行します。

手順



1. ナビゲーション領域で、**保守容易性**アイコンをクリックしてから、「**サービス管理**」を選択します。
2. コンテンツ・ペインで、「**Electronic Service Agent セットアップ・ウィザード**」を選択します。Electronic Service Agent ウィザードが開きます。ウィザードの指示に従い、コール・ホーム・タスクを構成します。

ユーザーの許可

Electronic Service Agent の許可要求を行います。Electronic Service Agent は、ご使用のシステムとユーザー ID とを関連付け、Electronic Service Agent 機能を介してシステム情報にアクセスできるようにします。この登録は、ご使用のオペレーティング・システムによって、AIX または IBM i オペレーション・システムのサービス・プロセスを自動化するためにも使用されます。

ユーザー ID を登録するには、以下のステップを完了します。



1. ナビゲーション領域で、**保守容易性**アイコンをクリックしてから、「**サービス管理**」を選択します。
2. コンテンツ・ペインで、「**ユーザーの許可**」をクリックします。
3. Electronic Service Agent に登録されたユーザー ID を入力します。ユーザー ID が必要な場合、[IBM 登録 Web サイト](#)で登録できます。
4. 「**了解**」をクリックします。

カスタマー・ユーザー ID の eService Web サイトへの登録について詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

Electronic Service Agent の使用可能化

このタスクは、管理対象システムのコール・ホーム状態を使用可能または使用不可にできるようにします。

注: この HMC で「カスタマイズ可能データ複製」が使用可能な場合 (「データ複製の管理」タスクを使用)、このタスクで指定されたデータは、ネットワーク上で構成されている他の HMC からの自動複製に応じて、変わる場合があります。データの複製について詳しくは、[84 ページの『データ複製の管理』](#)を参照してください。

管理対象システムのコール・ホーム状態を使用可能化にすることによって、サービス可能イベントが発生したとき、コンソールは自動的にサービス・センターに連絡するようになります。管理対象システムが使用不可の場合は、サービス担当員はサービス可能イベントについて通知されません。

システムのコール・ホームを管理するには:



1. ナビゲーション領域で、**保守容易性アイコン** をクリックしてから、「**サービス管理**」を選択します。
2. コンテンツ・ペインで、「**Electronic Service Agent の使用可能化**」をクリックします。
3. 「**Electronic Service Agent の使用可能化**」ウィンドウで、コール・ホーム状態を使用可能または使用不可にするシステムを 1 つまたは複数選択します。
4. タスクを終了したら、「**了解**」をクリックします。

Electronic Service Agent の使用可能化について詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

アウトバウンド接続の管理

ハードウェア管理コンソール (HMC) がリモート・サービスへの接続に使用するアウトバウンド接続の方法をカスタマイズします。

注: この HMC で「カスタマイズ可能データ複製」が使用可能な場合 (「データ複製の管理」タスクを使用)、このタスクで指定されたデータは、ネットワーク上で構成されている他の HMC からの自動複製に応じて、変わる場合があります。データの複製について詳しくは、[84 ページの『データ複製の管理』](#)を参照してください。

この HMC を構成して、接続をローカル・モデム、インターネット、インターネット仮想プライベート・ネットワーク (VPN)、またはリモート・パススルー・システムから試行するようにできます。リモート・サービスは、自動サービス・オペレーションを実行するための HMC と IBM サービス・サポート・システム間の両方向通信です。この接続は、HMC からのみ開始できます。IBM サービス・サポート・システムからは HMC との接続を開始できないだけでなく、開始しようとすることもありません。

接続情報をカスタマイズするには、以下の手順を実行します。



1. ナビゲーション領域で、**保守容易性アイコン** をクリックしてから、「**サービス管理**」を選択します。
2. コンテンツ・ペインで、「**アウトバウンド接続の管理 (Manage Outbound Connectivity)**」をクリックします。
3. タスクを進捗させる前に、「**アウトバウンド接続の管理**」ウィンドウで「**ローカル・サーバーをコール・ホーム・サーバーとして使用可能にする (Enable local server as call-home server)**」を選択します (チェック・マークが表示されます)。

注: 最初に、このタスクで指定した情報について記述された条件に同意する必要があります。

これによって、ローカル HMC が、コール・ホーム要求に関してサービス・プロバイダーのリモート・サポート機能に接続できるようになります。

4. ダイアル情報ウィンドウには、入力用の次のタブがあります。

- ローカル・モデム
 - インターネット (Internet)
 - インターネット VPN
 - パススルー・システム
5. モデム経由の接続を可能にする場合、「ローカル・モデム」タブで「サービスに対するローカル・モデム・ダイヤリングを許可する」を選択します。
 - a. ユーザーのロケーションから外線に接続するとき、最初に指定された番号 (プレフィックス) をダイヤルする必要がある場合は、「**モデムの構成 (Modem Configuration)**」をクリックし、「**モデム設定のカスタマイズ**」ウィンドウにロケーションに必要な「**アクセス番号**」を入力します。「**了解**」をクリックして設定を確定します。
 - b. 「ローカル・モデム」タブの「**追加 (Add)**」をクリックして、電話番号を追加します。ローカル・モデムのダイヤリングを可能にする場合、少なくとも 1 つの電話番号を構成する必要があります。
 6. インターネット経由の接続を可能にする場合、「インターネット」タブで「サービス用に既存のインターネット接続を許可 (**Allow an existing internet connection for service**)」を選択します。
 7. ローカル HMC からサービス・プロバイダーのリモート・サポート機能に接続するように、既存のインターネット接続上で VPN の使用を構成したい場合、「**インターネット VPN**」タブを使用します。
 8. HMC が TCP/IP アドレスまたはホスト名によって構成されるパススルー・システムを使用できるようにする場合は、「**パススルー・システム**」タブを使用します。
 9. 必要なフィールドにすべて入力したら、「**了解**」をクリックして変更を保管します。
- アウトバウンド接続情報のカスタマイズについて詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

インバウンド接続の管理

ハードウェア管理コンソール (HMC) などのローカル・コンソール、または管理対象システムの区画に、サービス・プロバイダーが一時的にアクセスできるようにする方法について説明します。

インバウンド接続を管理するには、次の手順を完了します。



1. ナビゲーション領域で、**保守容易性アイコン**  をクリックしてから、「**サービス管理**」を選択します。
2. コンテンツ・ペインで、「**インバウンド接続の管理**」をクリックします。
3. 「**インバウンド接続の管理**」設定ウィンドウから、以下のタスクを実行できます。
 - 「**リモート・サービス**」タブを使用して、手動リモート・サービス・セッションを開始するために必要な情報を指定します。
 - 「**呼び出し応答**」タブを使用して、サービス・プロバイダーからの着呼を受け入れるために必要な情報を指定し、自動リモート・サービス・セッションを開始します。
4. 「**了解**」をクリックして選択を続けます。

このタスクについて詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

カスタマー情報の管理

このタスクによって、ハードウェア管理コンソール (HMC) のカスタマー情報のカスタマイズが可能になります。

注: この HMC で「カスタマイズ可能データ複製」が使用可能な場合 (「**データ複製の管理**」タスクを使用)、このタスクで指定されたデータは、ネットワーク上で構成されている他の HMC からの自動複製に応

じて、変わる場合があります。データの複製について詳しくは、[84 ページの『データ複製の管理』](#)を参照してください。

「**カスタマー情報の管理 (Manage Customer Information)**」ウィンドウには、入力用の次のタブが表示されます。

- 管理者
- システム
- アカウント

カスタマー情報をカスタマイズするには、以下の手順を実行します。



1. ナビゲーション領域で、**保守容易性アイコン**  をクリックしてから、「**サービス管理**」を選択します。
2. コンテンツ・ペインで、「**カスタマー情報の管理**」をクリックします。
3. 「**カスタマー情報の管理 (Manage Customer Information)**」ウィンドウの「**管理者**」ページに該当する情報を入力します。
注: アスタリスク (*) の付いたフィールドは入力が必要です。
4. 「**カスタマー情報の管理 (Manage Customer Information)**」ウィンドウの「**システム**」と「**アカウント**」タブを選択して、追加情報を入力します。
5. タスクを終了したら、「**了解**」をクリックします。

アカウント情報のカスタマイズの詳細については、オンライン・ヘルプを利用してください。

イベント通知の管理

このタスクは、ご使用のシステムで問題イベントが発生した場合に、通知を受ける電子メール・アドレスを追加したり、どのような方法で Electronic Service Agent からシステム・イベントに関する通知を受け取るかを構成したりします。

通知をセットアップするには、以下の手順を実行します。



1. ナビゲーション領域で、**保守容易性アイコン**  をクリックしてから、「**サービス管理**」を選択します。
2. コンテンツ・ペインで、「**イベント通知の管理**」をクリックします。
3. 「**イベント通知の管理**」ウィンドウでは、以下のタスクを実行できます。
 - 「**電子メール**」タブを使用して、ご使用のシステムに問題イベントが発生した際、およびシステムでスケジュール操作が計画されている場合に通知する電子メール・アドレスを追加します。
 - 「**SNMP トラップ構成**」タブを使用し、ハードウェア管理コンソール (HMC) アプリケーション・プログラミング・インターフェース・イベント用の Simple Network Management Protocol (SNMP) トラップ・メッセージを送信するためのロケーションを指定します。
4. このタスクを終了したら、「**了解**」をクリックします。

このタスクについて詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

接続のモニタリング管理

障害を検出するために接続のモニタリングで使用するタイマーを構成し、選択したマシンに対して接続のモニタリングを使用可能または使用不可にする方法について説明します。

接続のモニタリング設定は、マシンごとに表示または変更 (権限がある場合) を行うことができます。HMC と管理対象システムとの間で通信上の問題が検出されると、接続モニタリング機能によりサービス可能イベントが生成されます。接続のモニタリングを使用不可にすると、選択したマシンとこの HMC との間のネットワークの問題に対してサービス可能イベントは生成されません。

接続をモニターするには、以下の手順を実行します。



1. ナビゲーション領域で、**保守容易性アイコン** をクリックしてから、「**サービス管理**」を選択します。
2. コンテンツ・ペインで、「**接続モニターの管理**」をクリックします。
3. 「**接続モニターの管理 (Manage Connection Monitoring)**」ウィンドウで、必要な場合タイマー設定を調整し、サーバーを使用可能または使用不可にします。
4. タスクを終了したら、「**了解**」をクリックします。

接続のモニタリングについて詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

リモート・オペレーション

ハードウェア管理コンソール (HMC) にリモート側で接続し、使用します。

リモート・オペレーションでは、ローカル HMC オペレーターが使用する GUI または HMC 上のコマンド行インターフェース (CLI) が使用されます。オペレーションはリモート側で以下の方法で実行できます。

- リモート HMC の使用。
- Web ブラウザーを使用してローカル HMC に接続。
- HMC リモート・コマンド行の使用。

「リモート HMC」は、サービス・プロセッサと異なるサブネット上にある HMC です。したがってサービス・プロセッサを IP マルチキャストによって自動ディスカバリーすることはできません。

リモート HMC またはローカル HMC に接続されている Web ブラウザーのどちらを使用するか決定する場合は、必要な制御範囲を検討してください。リモート HMC は、リモート HMC によって直接制御される管理対象オブジェクトの特定のセットを定義し、一方ローカル HMC に接続される Web ブラウザーは、ローカル HMC と同じ管理対象オブジェクトのセットを制御します。通信の接続性および通信速度も検討事項です。LAN 接続の場合、リモート HMC または Web ブラウザー制御について満足できる通信が可能になります。

リモート HMC の使用

リモート HMC は、完全な HMC のため、ほとんど完全な機能のセットを備えます。管理対象オブジェクトの構成プロセスのみローカル HMC と異なります。

リモート HMC は完全な HMC として、ローカルのハードウェア管理コンソールと同じセットアップおよびメンテナンス要件があります。リモート HMC は、管理する各管理対象オブジェクト (サービス・プロセッサ) との間に LAN TCP/IP 接続が必要です。したがって、リモート HMC とその管理対象オブジェクトとの間にカスタマー・ファイアウォールがあればいずれも、HMC からサービス・プロセッサへの通信を許可する必要があります。リモート HMC は、サービスおよびサポートのため別の HMC と通信することも必要になる場合があります。[109 ページの表 10](#) に、通信のためリモート HMC が使用するポートを示します。

表 10. リモート HMC が通信に使用するポート	
ポート	使用
udp 9900	HMC ツー HMC ディスカバリー
tcp 9920	HMC ツー HMC コマンド

リモート HMC は、サービスおよびサポートのため IBM (または IBM に接続されている別の HMC) との接続が必要です。IBM との接続は、インターネットの接続の形式 (企業のファイアウォール経由) を使用できます。

状況情報およびサービス・プロセッサの制御機能にアクセスする場合のパフォーマンスと可用性は、リモート HMC と管理対象オブジェクトを接続するカスタマー・ネットワークの信頼性、可用性、および応答性によって変わります。リモート HMC は、各サービス・プロセッサとの接続をモニターし、逸失した接続をリカバリーしようとし、またリカバリーできない接続の報告も可能です。

リモート HMC のセキュリティは、HMC ユーザー・ログオン手順によってローカル HMC と同じ方法で確保されます。リモート HMC と各サービス・プロセッサ間の通信は、ローカル HMC と同様に暗号化されます。セキュアな通信のための認証が提供され、必要であれば、ユーザーによる変更も可能です。

リモート HMC への TCP/IP アクセスは、リモート HMC が内部で管理するファイアウォールによって制御され、HMC 関連機能に限定されます。

Web ブラウザーの使用

単一のローカル・ハードウェア管理コンソール (HMC) に接続した管理対象オブジェクトの不定期なモニターと制御が必要な場合は、Web ブラウザーを使用します。Web ブラウザーの使用例として、オペレーターまたはシステム・プログラマーが時間外に自宅からモニターする場合があります。

各 HMC には、指定したユーザーのセットからリモート・アクセスできるように構成可能な Web サーバーが含まれています。Web ブラウザーとローカル HMC の間にお客様のファイアウォールが存在する場合は、ポートがアクセス可能であり、ファイアウォールがこれらのポートへの着信要求を許可するようセットアップされる必要があります。[110 ページの表 11](#) では、Web ブラウザーで HMC との通信に必要なポートを示します。

表 11. Web ブラウザーが HMC への通信に使用するポート	
ポート	使用
TCP 443	セキュア (HTTPS) リモート・インターフェース 通信
TCP 8443	ブラウザーから Web サーバーにアクセスするセキュア通信
TCP 9960	ブラウザー・アプレット通信
¹ このポートは、HMC バージョン 7.8.0 以降でリモート・アクセスが使用可能になっている場合は、HMC ファイアウォールで開かれています。このポートは、リモート・クライアントと HMC との間にある、どのファイアウォールでも開かれている必要があります。	

HMC を構成して Web ブラウザー・アクセスを可能にすると、有効なユーザーは Web ブラウザーから、ローカル・ディスクまたは DVD メディアなど HMC への物理アクセスが必要な機能を除いて、ローカル HMC に構成されたすべての機能にアクセスできます。リモート Web ブラウザーに提供されるユーザー・インターフェースは、ローカル HMC のユーザー・インターフェースと同じで、ローカル HMC と同じ制約が適用されます。

Web ブラウザーは、LAN TCP/IP 接続および暗号化 (HTTPS) プロトコルのみを使用して、ローカル HMC に接続できます。Web ブラウザーのログオン・セキュリティは、HMC ユーザー・ログオン手順によって確保されます。セキュアな通信のための認証が提供され、ユーザーによる変更も可能です。

状況情報および管理対象オブジェクトの制御機能にアクセスする場合のパフォーマンスと可用性は、Web ブラウザーとローカル HMC を接続するネットワークの信頼性、可用性、および応答性によって変わります。Web ブラウザーと個々の管理対象オブジェクトは直接接続されているわけではないため、Web ブラウザーは各サービス・プロセッサへの接続のモニター、リカバリー、および接続逸失の報告は行いません。これらの機能は、ローカル HMC が処理します。

Web ブラウザー・システムは、サービスまたはサポートのために IBM と接続する必要はありません。ブラウザーとシステム・レベルのメンテナンスはお客様の責任となります。

HMC の URL を `https://xxx.xxx.xxx.xxx (xxx.xxx.xxx.xxx は IP アドレス)` 形式で指定し、Microsoft Internet Explorer をブラウザーとして使用すると、ホスト名不一致のメッセージが表示されます。このメッセージ

を回避するには Firefox ブラウザーを使用するか、ホスト名を「**ネットワーク設定の変更**」タスクを使用して HMC 用に構成します (77 ページの『**ネットワーク設定の変更**』を参照)。このホスト名は IP アドレスでなく URL で指定されます。例えば、`https://host name.domain_name` または `https://host name` の形式を使用できます (`https://hmc1.ibm.com` または `https://hmc1` など)。

Web ブラウザーを使用するための準備

Web ブラウザーを使用したハードウェア管理コンソール (HMC) へのアクセスを準備するために必要なステップを実行します。

Web ブラウザーを使用して HMC にアクセスする前に、以下のタスクを実行する必要があります。

- HMC を、指定したユーザーがリモート制御できるように構成します。
- LAN ベース接続の場合、制御する HMC の TCP/IP アドレスを認識し、その HMC と Web ブラウザーとの間のファイアウォール・アクセスを正しく設定する必要があります。
- HMC Web アクセスのために、有効なユーザー ID およびパスワードをアクセス管理者に割り当ててもらいます。

Web ブラウザーの要件

ハードウェア管理コンソール (HMC) のモニターと制御を行うために Web ブラウザーが満たす必要がある要件について説明します。

HMC Web ブラウザー・サポートには、HMC に接続するブラウザーで HTML 2.0、JavaScript1.0、Java™ 仮想マシン (JVM)、Java Runtime Environment (JRE) バージョン 7 および Cookie サポートが必要です。お使いのブラウザーで Java 仮想マシンが構成されているかどうか判別する場合は、サポート担当員にお問い合わせください。Web ブラウザーは HTTP 1.1 を使用する必要があります。プロキシ・サーバーを使用している場合、プロキシ接続用に HTTP 1.1 が使用可能になっていることが必要です。さらに、ブラウザーがポップアップを使用不可にして実行されている場合、ブラウザーでアドレス指定されているすべての HMC について、ポップアップを使用可能にする必要があります。テスト済みのブラウザーは、次のとおりです。

Google Chrome

HMC バージョン 8.1 は Google Chrome バージョン 33 をサポートします。

Microsoft Internet Explorer

HMC バージョン 8.1 は Internet Explorer 9.0、Internet Explorer 10.0、および Internet Explorer 11.0 をサポートします。

注：パフォーマンス CEC タスクは、Internet Explorer 9.0 ではサポートされません。

- ご使用のブラウザーがインターネット・プロキシを使用するように構成されている場合は、例外リストにローカル IP アドレスが含まれています。詳しくは、お客様のネットワーク管理者にお問い合わせください。ハードウェア管理コンソールにアクセスするのにどうしてもプロキシを使用する必要がある場合は、「インターネット オプション」ウィンドウの「**詳細設定**」タブで「**プロキシ接続で HTTP 1.1 を使用する**」を使用可能にします。

Mozilla Firefox

HMC バージョン 8.1 は Mozilla Firefox バージョン 17 および Mozilla Firefox バージョン 24 延長サポート版 (Extended Support Release (ESR)) をサポートします。ウィンドウのフォーカス (前面か背面か) の切り替え、および既存のウィンドウを移動またはサイズ変更する JavaScript オプションが使用可能になっているかを確認します。これらのオプションを使用可能にするには、ブラウザーの「Options」ダイアログにある「**コンテンツ**」タブをクリックし、「JavaScript を有効にする」オプションの隣にある「**詳細設定**」をクリックします。次に、「ウィンドウのフォーカス (前面か背面か) を切り替える」オプションおよび「ウィンドウの移動または大きさの変更」オプションを選択します。これらのオプションを使用して、HMC タスク間の切り替えを容易にします。最新の Mozilla Firefox ESR レベルについて詳しくは、『**Firefox ESR セキュリティアドバイザリ**』を参照してください。

注：HMC が NIST SP 800-131a セキュリティ・モードになっているときに Mozilla Firefox を使用している場合は、以下の制約事項が適用されます。

- Mozilla Firefox をリモート・クライアントに使用することはできません。

- ローカル・コンソールを使用することはできません。

他の Web ブラウザーの考慮事項

リモート側で HMC に接続時に ASMI が作動するには、セッション Cookie を使用可能にする必要があります。ASM プロキシ・コードはセッション情報を保管し、その情報を使用します。

Internet Explorer

1. 「ツール」 > 「インターネット オプション」をクリックします。
2. 「プライバシー」タブをクリックし、「詳細設定」を選択します。
3. 「すべての Cookie を受け入れる」にチェック・マークが付いていることを確認します。
4. チェック・マークが付いていない場合は、「自動 Cookie 処理を上書きする」および「常にセッション Cookie を許可する」を選択します。
5. 「ファーストパーティの Cookie」および「サードパーティの Cookie」については、「ブロックする」、「ダイアログを表示する」、または「受け入れる」を選択します。「ダイアログを表示する」を選択することが推奨されます。この場合、あるサイトが Cookie を書き込む都度、プロンプトが出されます。一部のサイトは Cookie の書き込みを許可される必要があります。

Firefox

1. 「ツール」 > 「Options」をクリックします。
2. 「Cookie」タブをクリックします。
3. 「Allow sites to set cookies」を選択します。
4. 特定のサイトだけ許可したい場合、「Exceptions」を選択してから、アクセスを許可するためにこの HMC を追加します。

HMC リモート・コマンド行の使用

HMC グラフィカル・ユーザー・インターフェースでタスクを実行するための代替方法は、コマンド行インターフェース (CLI) を使用することです。

コマンド行インターフェースは、次の状態で使用できます。

- 整合性のある結果が必要であるとき。いくつかの管理対象システムを管理しなければならない場合、コマンド行インターフェースを使用することにより整合性のある結果を得ることができます。コマンド文字列はスクリプトで保管され、リモート側で実行することができます。
- 自動化された操作が必要であるとき。管理対象システムを管理するための整合性のある方法を作成した後、他のシステムから、クローン・デーモンなどのバッチ処理アプリケーションでスクリプトを開始することにより、操作を自動化することができます。

ローカル HMC では、コンソール・ウィンドウでコマンド行インターフェースを使用できます。

SSH クライアントと HMC 間のセキュアなスクリプト実行のセットアップ

セキュア・シェル (SSH) クライアントとハードウェア管理コンソール (HMC) 間のスクリプト実行は確実にセキュアにする必要があります。

HMC は、通常、管理対象システムがあるサーバー室に配置されるので、HMC に物理的に近寄ることができない場合があります。この場合は、リモート Web ブラウザーまたはリモート・コマンド行インターフェースを使用して、リモート側からアクセスできます。

注: SSH クライアントと HMC 間でスクリプトを無人で実行できるようにするには、SSH プロトコルをクライアントのオペレーティング・システム上にインストールしておく必要があります。

SSH クライアントと HMC 間でスクリプトを無人で実行できるようにするには、以下の手順を完了します。

1. リモート・コマンド実行を使用可能にします。詳しくは、[100 ページの『リモート・コマンド実行を有効にする』](#)を参照してください。
2. クライアントのオペレーティング・システムで、SSH プロトコル鍵生成プログラムを実行します。SSH プロトコル鍵生成プログラムを実行するには、以下の手順を完了します。

- a. キーを保管するには、`$HOME/.ssh` という名前のディレクトリーを作成します (RSA または DSA のいずれかのキーを使用できます)。
- b. 公開鍵および秘密鍵を生成するには、次のコマンドを実行します。

```
ssh-keygen -t rsa
```

`$HOME/.ssh` ディレクトリーに次のファイルが作成されます。

```
private key: id_rsa
public key: id_rsa.pub
```

group および other の両方の書き込みビットがオフになります。秘密鍵の許可が 600 になっていることを確認します。

3. クライアントのオペレーティング・システム上で、以下のコマンドを使用することにより、SSH を使用し、`mkauthkeys` コマンドを実行して、HMC 上の HMC ユーザーの `authorized_keys2` ファイルを更新します。

```
ssh hmcuser@hmchostname mkauthkeys --add <the contents of $HOME/.ssh/
id_rsa.pub>
```

注: リモート・シェルが適切にコマンドを処理できるようにするために、コマンド内で二重引用符 (") が使用されます。例:

```
ssh "mkauthkeys hscuser@somehmc host --add 'ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDA+Zc8+hn1+
TjEXu640LqnVNB+UsixIE3c649Cgj20gaVWnFKTjcpWVahK/duCLac/zteMtVAfCx7/ae2g5RTPu7FudF2xjs4r
+NadVXhoIqmA53a
NjE4GILpfe5v0F25xkBdG9wxigGtJy0KeJHzgnElP7RlEe0BijJDKo5gGE12NVfBxboChm6LtKnDxLi9ahh0YtLlFehJr
6pV/1MAEu
Lhd6ax1hWwvrf/
h5Ym6J8JbLVL3EeKbCsuG9E4iN1z4HrPkT50QLqtvc1A1jch1ravsaQqYl0MTWNFz4M4Qo503fZbLc6RuJjtJv8C5t
4/SZUGHZxSPnQmku1i1z9hxt hscpe@vmcccloudvm179'"
```

HMC から鍵を削除するには、次のコマンドを使用します。

```
ssh hmcuser@hmchostname mkauthkeys --remove joe@somehost
```

SSH を介して HMC にアクセスするすべてのホストに対してプロンプトが出されるパスワードを使用可能にするには、次のように `scp` コマンドを使用して HMC からの鍵ファイルをコピーします。 `scp hmcuser@hmchostname:~/.ssh/authorized_keys2 authorized_keys2`

次のように、`authorized_keys2` ファイルを編集し、このファイル内のすべての行を除去してから、それを HMC にコピーし直します。 `scp authorized_keys2 hmcuser@hmchostname:~/.ssh/authorized_keys2`

HMC リモート・コマンドの使用可能および使用不可設定

ハードウェア管理コンソール (HMC) にアクセスするリモート・コマンド行インターフェースを使用可能または使用不可にできます。

リモート・コマンドを使用可能または使用不可にするには、以下の手順を実行します。

1. ナビゲーション領域で、管理対象システムを選択し、「ユーザーおよびセキュリティ」アイコン  をクリックしてから、「ユーザーおよびロール」を選択します。
2. コンテンツ・ペインで、「リモート・コマンド実行を有効にする」をクリックします。
3. 「リモート・コマンド実行を有効にする」ウィンドウで、以下のオプションから選択します。
 - リモート・コマンドを使用可能にするには、「ssh 機能を使用してリモート・コマンド実行を可能にする」を選択します。
 - リモート・コマンドを使用不可にするには、「ssh 機能を使用してリモート・コマンド実行を可能にする」が選択されていないことを確認します。
4. 「了解」をクリックします。

LAN 接続 Web ブラウザーからの HMC のログイン

LAN 接続 Web ブラウザーから、ハードウェア管理コンソール (HMC) にリモート側でログインします。

LAN 接続 Web ブラウザーから HMC にログインするには、次のステップを実行します。

1. ご使用の Web ブラウザーが目的の HMC に LAN 接続できることを確認してください。
2. ご使用の Web ブラウザーから、希望する HMC の URL を形式 `https://hostname.domain_name` (for example: `https://hmc1.ibm.com`) または `https://xxx.xxx.xxx.xxx` で入力します。

この接続が、現在の Web ブラウザー・セッションでその HMC への初めてのアクセスである場合は、認証エラーを受け取る場合があります。この認証エラーは、以下のいずれかの条件が発生した場合に表示されます。

- HMC に含まれる Web サーバーが自己署名証明書を使用するように構成され、ブラウザーが HMC を証明書の発行者としてトラストするように構成されていない場合。
- HMC が認証局 (CA) の署名による証明書を使用するように構成され、ブラウザーがこの CA をトラストするように構成されていない場合。

どちらの場合も、ブラウザーに表示される証明書が HMC で使用する証明書であることがわかっていれば、続行することができ、HMC へのすべての通信は暗号化されます。

どのブラウザー・セッションでも最初のアクセスで証明書エラー通知を受け取らないようにするには、ブラウザーが HMC または CA をトラストするように構成します。一般にブラウザーを構成するには、次のいずれかの方法を使用します。

- ブラウザーが証明書の発行者を永続的にトラストするように指示する必要があります。
- 証明書を表示し、トラステッド CA のデータベースにインストールすることにより、証明書を発行する CA の証明書が HMC によって使用されます。

証明書が自己署名の場合、HMC 自体が証明書を発行する CA として認識されます。

3. プロンプトが出されたら、管理者から割り当てられたユーザー名とパスワードを入力します。

HMC を使用した OpenBMC ベースのシステムおよび BMC ベースのシステムの管理

ハードウェア管理コンソール (HMC) を使用して OpenBMC ベースのシステムおよび BMC ベースのシステムを管理する方法について説明します。

このタスクについて

コンソールから実行するタスクと、管理対象システムのグラフィカル・ビューおよび簡易ナビゲーションを備えた Web ベースのユーザー・インターフェースを使用してベースボード管理コントローラー (BMC) をナビゲートする方法について説明します。

注: HMC が NIST モードで稼働しているときには、OpenBMC ベースのシステムおよび BMC ベースのシステムを管理することはできません。

管理対象システムの追加

管理対象のベースボード管理コントローラー (BMC) システムをハードウェア管理コンソール (HMC) に追加する方法について説明します。

- 1 つ以上の管理対象 BMC システムを HMC に追加するには、以下のステップを実行します。

1. HMC ダッシュボードから、「システムの接続」をクリックします。
2. 「管理対象システムの追加」ウィンドウから、以下のフィールドに入力することで BMC システムを追加できます。
 - IP アドレス/ホスト名
 - ユーザー名 (BMC システム)

注:

- モデル 8335-GTH および 8335-GTX の場合、デフォルト・ユーザー名は admin です。
- モデル 9006-12P および 9006-22P の場合、デフォルト・ユーザー名は ADMIN です。

・パスワード

あるいは、IP アドレスの範囲を指定して「**OK**」をクリックして、検出されたシステムのリストを表示することもできます。検出されたシステムを 1 つ以上選択して、HMC に追加することができます。

注: ディスカバリー・プロセスは、完了するまでに長時間かかる場合があります。

3. 「**OK**」をクリックして、管理対象システムを HMC に追加します。

このタスクについて詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

システム管理 (サーバー)

「システム管理」には、サーバーを管理するためのタスクが表示されます。これらのタスクを使用して、サーバーのセットアップ、構成、状況の表示、トラブルシューティング、およびソリューションの適用を行います。

これらのタスクは、管理対象システムが選択されたときにリストされます。メニュー・ポッドにリストされるタスクは、作業域で選択を行うと変わります。

操作

「操作」には、管理対象システムを操作するためのタスクが含まれています。

電源オフ

管理対象システムをシャットダウンします。

以下のオプションから選択してください。

通常の電源オフ

「通常の電源オフ」モードは、制御された方法でシステムの操作をシャットダウンします。シャットダウンの間、アクティブなジョブで実行されているプログラムは、クリーンアップ (ジョブ終了処理) を実行できます。

電源オン

「電源オン」タスクを使用して、管理対象システムを開始します。

以下のオプションから選択して、管理対象システムを電源オンします。

通常 (Normal): このオプションは、HMC が区画開始ポリシーの現行設定を使用して管理対象システムの電源オン方法を決定することを指定する場合に選択します。デフォルト設定は、以下の値に設定されます。

- ・ **常に自動開始 (Auto-Start Always):** このオプションは、管理対象システムの電源がオンになると HMC が自動的に論理区画を電源オンすることを指定します。管理対象システムの電源オンがユーザー・アクションの結果である場合、HMC は自動始動用に構成されたすべての区画を開始します。管理対象システムの電源が自動リカバリー・プロセスの結果オンになった場合、HMC は、システムが電源オフされたときに実行中だった論理区画のみを開始します。このオプションは常に選択可能です。

操作のスケジュール

オペレーターの介入なしで、管理対象システム上で実行する特定の操作のスケジュールを作成します。

システム操作の自動処理、遅延処理、または反復処理が必要な状況では、スケジュール操作が便利です。スケジュール操作は、指定した時刻に、オペレーターが操作の実行に携わることなく開始します。スケジュールには、1 回の操作または複数回の繰り返しを設定できます。

例えば、管理対象システムの電源オン/オフ操作をスケジュールできます。

「スケジュール操作」タスクは、各操作について次の情報を表示します。

- ・ 操作の対象になるプロセッサ

- スケジュールされている日付
- スケジュールされている時刻
- 操作
- 残されている繰り返し回数

「スケジュール操作」ウィンドウでは、以下のタスクを実行できます。

- 操作を後で実行するようスケジュールします。
- 操作を定期的な間隔で繰り返し実行するように定義します。
- スケジュール操作を削除します。
- 現在スケジュールされている操作の詳細を表示します。
- 指定した時刻範囲内にスケジュールされている操作を表示します。
- スケジュールされている操作を、日付、操作、または管理対象システム別にソートします。

ある操作が一度実行されるようにスケジュールするか、またはそれが繰り返し実行されるようにスケジュールすることができます。操作が実行される時刻および日付を指定する必要があります。操作を繰り返し実行させたい場合、以下のオプションを選択する必要があります。

- 操作を実行する曜日 (任意)
- 操作の実行間隔または時刻 (必須)
- 繰り返しの合計回数 (必須)

管理対象システムについてスケジュール可能な操作には、以下のものがあります。

管理対象システムの電源オフ

1つの管理対象システムに一定間隔でシステム電源オフにする操作をスケジュールします。

管理対象システムの電源オン

1つの管理対象システムに一定間隔でシステム電源オンにする操作をスケジュールします。

管理対象システム上の操作をスケジュールするには、以下のステップを完了します。



1. ナビゲーション領域で、リソース・アイコン  をクリックしてから、「すべてのサーバー」を選択します。
2. コンテンツ・ペインで、1つ以上の管理対象システムを選択します。
3. メニュー・ポッドで、「アクション」 > 「すべてのアクションの表示」 > 「操作」 > 「操作のスケジュール」を選択します。
4. 「操作のスケジュール」ウィンドウから、メニューバーの「オプション」をクリックし、オプションの次のレベルを表示します。
 - スケジュール操作を追加するには、「オプション」をクリックしてから「新規」をクリックします。
 - スケジュール操作を削除するには、削除する操作を選択して「オプション」を選択してから「削除」をクリックします。
 - 選択したオブジェクトについて、スケジュール操作のリストを現在のスケジュールで更新するには、「オプション」を選択してから「最新表示」をクリックします。
 - スケジュール操作を表示するには、表示する操作を選択して「表示」を選択してから「スケジュールの詳細」をクリックします。
 - スケジュール操作の時間を変更するには、変更する操作を選択して「表示」を選択してから「新しい時間範囲」をクリックします。
 - スケジュール操作をソートするには、「ソート」を選択してから表示されるソート・カテゴリーのいずれかをクリックします。
5. HMC ワークスペースに戻るには、「操作」を選択してから「終了」をクリックします。

BMC システム管理の起動

ハードウェア管理コンソール (HMC) は、選択したシステムのベースボード管理コントローラー (BMC) に直接接続することができます。

BMC システム管理はサービス・プロセッサとのインターフェースで、これにより電源の自動再始動などのサーバーの動作を管理したり、エラー・ログや重要プロダクト・データなどのサーバーに関する情報を表示したりできます。

BMC に接続するには、以下のステップを実行します。

注：BMC ユーザー・インターフェースにアクセスするには、コンソールからアクセスするか、サポートされる Web ブラウザーを使用して BMC にアクセスする必要があります。



1. ナビゲーション領域で、リソース・アイコン  をクリックしてから、「すべてのサーバー」を選択します。
2. コンテンツ・ペインで、1 つ以上の管理対象システムを選択します。
3. メニュー・ポッドで、「アクション」 > 「すべてのアクションの表示」 > 「操作」 > 「**BMC システム管理の起動 (Launch BMC System Management)**」を選択します。
4. 「続行」をクリックします。

コール・ホームの構成

BMC ベースの管理対象システム上の問題は、ハードウェア管理コンソール (HMC) にイベントとして報告されます。任意のイベントについて、自動的にアラートが通知されるようにセットアップすることができます。

注：アラートを受け取るには、HMC で SNMP トラップを有効にする必要があります。SNMP トラップを有効にするには、「コンソール設定」 > 「ネットワーク設定の変更」 > 「LAN アダプター」 > 「詳細」 > 「ファイアウォール設定」にナビゲートします。表から「SNMP トラップ」および「SNMP エージェント」を選択し、「着信の許可」をクリックします。

コール・ホームのアラートをセットアップするには、以下のステップを実行します。

注：この手順は、モデル 9006-12P、9006-22C、および 9006-22P に適用できます。

1. 「**BMC システム管理 (BMC System Management)**」ウィンドウから、「構成」 > 「アラート」をクリックします。
2. 表から任意のアラートを選択して、「変更」をクリックします。

注：複数の HMC をセットアップして、トラップを受け取ることができます。重複するイベントの検証は実行されないため、複数の HMC によってイベントの報告が重複する可能性があります。

3. 以下のフィールドをすべて入力します。

- ・ イベントの重大度
- ・ 宛先 IP

4. 「保管」をクリックします。
5. 表で新規アラートを確認します。

このタスクについて詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

再ビルド

管理対象システムから構成情報を抽出し、ハードウェア管理コンソール (HMC) 上に情報を再ビルドすることができます。

このタスクによって、実行中のサーバーの操作が中断されることはありません。

管理対象システムを再ビルドすると、その管理対象システムに関して HMC 上にある情報が更新されます。管理対象システムの再ビルドは、管理対象システムの状態が **Incomplete** (不完全) である場合に有用です。「**Incomplete**」の状態とは、管理対象システムの論理区画、プロファイル、またはリソースから、HMC が完全な情報を収集できない状態を意味します。

管理対象システムの再ビルドは、**HMC** ウィンドウを最新表示するのとは異なります。管理対象システムが再ビルドされると、HMC は管理対象システムから情報を抽出します。HMC が管理対象システムを再ビルドしている間は、他のタスクを開始できません。このプロセスには数分かかることがあります。

更新

システム情報の表示、ご使用のハードウェア管理コンソール (HMC) での更新の管理、またはシステムの作動可能確認を行うためのタスクを表示します。

ライセンス内部コードの変更

ハードウェア管理コンソール (HMC) を使用して、管理対象 BMC システムのライセンス内部コードを変更します。

システム・ファームウェアは、BMC ファームウェアと PNOR ファームウェアの組み合わせです。システムが適切に作動するためには、BMC ファームウェアと PNOR ファームウェアの両方を更新する必要があります。一方のファームウェアのみを更新し、他方のファームウェアを更新しないと、システム・エラーが発生する可能性があります。

ライセンス内部コードを変更するには、以下の手順を完了します。

1. ナビゲーション領域で、リソース・アイコン  をクリックしてから、「すべてのサーバー」を選択します。
2. システム情報を表示したいサーバーを選択します。
3. メニュー・ポッドで、「アクション」を展開し、次に、「更新」を展開します。
4. 「ライセンス内部コードの変更」>「BMC ライセンス内部コードの変更 (BMC Change Licensed Internal Code)」を選択します。
5. 「BMC ライセンス内部コードの変更 (BMC Change Licensed Internal Code)」ガイド付きウィザードで、画面に示される手順に従います。

注：ウィザードを進める前に、BMC システムを電源オフ状態にする必要があります。

6. このタスクを完了したら、「閉じる」をクリックします。

このタスクについて詳細な情報が必要な場合は、オンライン・ヘルプを使用してください。

アテンション LED

管理対象システム上でのシステム・アテンション LED 情報の表示、特定の LED の点灯によるシステム・コンポーネントの識別、およびすべての LED のテストを行います。

システムは、エンクロージャーや現場交換可能ユニット (FRU) など、システム内のさまざまなコンポーネントを識別するのに役立ついくつかの LED を備えています。この理由から、これらの LED は**識別 LED**と呼ばれます。個々の LED は、コンポーネント上またはその近くにあります。LED は、コンポーネント自身かまたはコンポーネントのキャリア (例えば、メモリー・カード、ファン、メモリー・モジュール、またはプロセッサ) に付いています。LED は緑色またはオレンジ色です。緑色の LED は、次のいずれかの状態を示します。

- 電源が入っている
- リンク上でアクティビティあり (システムが情報の送信または受信を行っている)

オレンジ色の LED は障害または識別状態を示します。システムまたはシステム上のいずれかのコンポーネントのオレンジ色の LED が点灯または明滅している場合は、問題を識別し、システムを正常な状態に戻すための適切な処置を行ってください。

ユーザーは、以下のタイプの識別 LED を活動化または非活動化することができます。

エンクロージャーの識別 LED

特定のドロワー (エンクロージャー) にアダプターを追加する場合、ドロワーのマシン・タイプ、モデル、およびシリアル番号 (MTMS) を知っておく必要があります。新規アダプターを必要とするドロワー

用の正しい MTMS を持っているかどうかを調べるには、ドロワーの LED を活動化して、MTMS が新規アダプターを必要とするドロワーに対応しているかどうかを確認することができます。

システム・アテンション LED を非活動化することができます。例えば、問題が優先度の高いものでないと判別し、その問題を後で修復する場合があります。ただし、別の問題が発生した場合はアラートを受け取りたいので、システム・アテンション LED を非活動化して、別の問題が発生したときに再度活動化できるようにする必要があります。

接続

サービス・プロセッサへのハードウェア管理コンソール (HMC) 接続状況の表示、これらの接続のリセット、選択した管理対象システムへの他の HMC の接続、または別の HMC の切断を行うことができます。

作業域で管理対象システムを選択した場合、以下のタスクがその管理対象システムに関連付けられます。

サービス・プロセッサの状況

管理対象システム上のサービス・プロセッサへのハードウェア管理コンソール (HMC) 接続の状況に関する情報を表示します。

このタスクについて

管理対象システムで、サービス・プロセッサへのサービス・プロセッサ接続状況を表示するには、以下の手順を完了します。

手順



1. ナビゲーション領域で、リソース・アイコン  をクリックしてから、「すべてのサーバー」を選択します。
2. サービス・プロセッサ接続状況を表示するサーバーを選択する。
3. メニュー・ポッドで、「アクション」 > 「すべてのアクションの表示」 > 「接続」 > 「サービス・プロセッサの状況」を選択します。

接続のリセットまたは除去

ハードウェア管理コンソール (HMC) インターフェースから、管理対象システムのリセットまたは除去を行います。

このタスクについて

接続をリセットまたは除去するには、次の手順を完了します。

手順



1. ナビゲーション領域で、リソース・アイコン  をクリックしてから、「すべてのサーバー」を選択します。
2. リセットまたは除去を行うサーバーを選択する。
3. メニュー・ポッドで、「アクション」 > 「すべてのアクションの表示」 > 「接続」 > 「接続のリセットまたは除去」を選択します。
4. 「接続のリセット」または「接続の除去」を選択します。
5. 「了解」をクリックします。

特記事項

本書は米国が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒 103-8510

東京都中央区日本橋箱崎町 19 番 21 号

日本アイ・ビー・エム株式会社

法務・知的財産

知的財産権ライセンス渉外

以下の保証は、国または地域の法律に沿わない場合は、適用されません。IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態を提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任は適用されないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Director of Licensing

IBM Corporation

North Castle Drive, MD-NC119

Armonk, NY 10504-1785

US

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

記載されている性能データとお客様事例は、例として示す目的でのみ提供されています。実際の結果は特定の構成や稼働条件によって異なります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する

る実行性、互換性、またはその他の要求については確証できません。IBM 以外の製品の性能に関する質問は、それらの製品の供給者をお願いします。

IBM の将来の方向または意向に関する記述は、予告なしに変更または撤回される場合があります、単に目標を示しているものです。

表示されている IBM の価格は IBM が小売り価格として提示しているもので、現行価格であり、通知なしに変更されるものです。卸価格は、異なる場合があります。

本書はプランニング目的としてのみ記述されています。記述内容は製品が使用可能になる前に変更になる場合があります。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、類似する個人や企業が実在しているとしても、それは偶然にすぎません。

著作権使用許諾:

本書には、様々なオペレーティング・プラットフォームでのプログラミング手法を例示するサンプル・アプリケーション・プログラムがソース言語で掲載されています。お客様は、サンプル・プログラムが書かれているオペレーティング・プラットフォームのアプリケーション・プログラミング・インターフェースに準拠したアプリケーション・プログラムの開発、使用、販売、配布を目的として、いかなる形式においても、IBM に対価を支払うことなくこれを複製し、改変し、配布することができます。このサンプル・プログラムは、あらゆる条件下における完全なテストを経ていません。従って IBM は、これらのサンプル・プログラムについて信頼性、利便性もしくは機能性があることをほのめかしたり、保証することはできません。サンプル・プログラムは特定物として現存するままの状態を提供されるものであり、いかなる保証も提供されません。IBM は、お客様の当該サンプル・プログラムの使用から生ずるいかなる損害に対しても一切の責任を負いません。

それぞれの複製物、サンプル・プログラムのいかなる部分、またはすべての派生的創作物にも、次のように、著作権表示を入れていただく必要があります。

© (お客様の会社名) (西暦年).

このコードの一部は、IBM Corp. のサンプル・プログラムから取られています。

© Copyright IBM Corp. _年を入れる_.

この情報をソフトコピーでご覧になっている場合は、写真やカラーの図表は表示されない場合があります。

IBM Power Systems サーバーのアクセシビリティ機能

アクセシビリティ機能は、運動障害または視覚障害など身体に障害を持つユーザーが情報技術コンテンツを快適に使用できるようにサポートします。

概説

IBM Power Systems サーバーには、次の主なアクセシビリティ機能が組み込まれています。

- キーボードのみによる操作
- スクリーン・リーダーを使用する操作

IBM Power Systems サーバーでは、最新の W3C 標準 [WAI-ARIA 1.0](http://www.w3.org/TR/wai-aria/) (www.w3.org/TR/wai-aria/) が [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) および [Web Content Accessibility Guidelines \(WCAG\) 2.0](http://www.w3.org/TR/WCAG20/) (www.w3.org/TR/WCAG20/) に準拠するように使用されています。アクセシビリティ機能を利用するためには、最新リリースのスクリーン・リーダーに加えて、IBM Power Systems サーバーでサポートされている最新の Web ブラウザーを使用してください。

IBM Knowledge Center に用意されている IBM Power Systems サーバーのオンライン製品資料は、アクセシビリティに対応しています。IBM Knowledge Center のアクセシビリティ機能は、[IBM Knowledge Center のヘルプの『アクセシビリティ』セクション](http://www.ibm.com/support/knowledgecenter/help#accessibility) (www.ibm.com/support/knowledgecenter/help#accessibility) で説明されています。

キーボード・ナビゲーション

この製品では、標準ナビゲーション・キーが使用されています。

インターフェース情報

IBM Power Systems サーバーのユーザー・インターフェースには、1 秒当たり 2 回から 55 回明滅するコンテンツはありません。

IBM Power Systems サーバーの Web ユーザー・インターフェースは、コンテンツの適切なレンダリング、および使用可能なエクスペリエンスの提供を、カスケード・スタイル・シートに依存しています。アプリケーションは、視覚障害者が、ハイコントラスト・モードを含め、システム表示形式の設定を使用するために同等の仕組みを提供します。フォント・サイズの制御は、デバイスまたは Web ブラウザーの設定を使用して行うことができます。

IBM Power Systems サーバーの Web ユーザー・インターフェースには、アプリケーションの機能領域に迅速にナビゲートできる WAI-ARIA ナビゲーション・ランドマークが組み込まれています。

ベンダー・ソフトウェア

IBM Power Systems サーバーには、IBM の使用許諾契約書の適用外である特定のベンダー・ソフトウェアが組み込まれています。IBM では、それら製品のアクセシビリティ機能については、何ら保証責任を負いません。ベンダーの製品に関するアクセシビリティ情報については、該当のベンダーにお問い合わせください。

関連したアクセシビリティ情報

標準の IBM ヘルプ・デスクおよびサポートの各 Web サイトに加え、IBM では、聴覚障害を持つユーザーまたは聴覚機能が低下しているユーザーが販売サービスやサポート・サービスにアクセスするのに使用できる TTY 電話サービスを用意しています。

TTY サービス
800-IBM-3383 (800-426-3383)
(北アメリカ内)

アクセシビリティに対する IBM の取り組みについて詳しくは、[IBM アクセシビリティ \(www.ibm.com/able\)](http://www.ibm.com/able) を参照してください。

プライバシー・ポリシーに関する考慮事項

サービス・ソリューションとしてのソフトウェアも含めた IBM ソフトウェア製品（「ソフトウェア・オファリング」）では、製品の使用に関する情報の収集、エンド・ユーザーの使用感の向上、エンド・ユーザーとの対話またはその他の目的のために、Cookie をはじめさまざまなテクノロジーを使用することがあります。多くの場合、ソフトウェア・オファリングにより個人情報が収集されることはありません。IBM の「ソフトウェア・オファリング」の一部には、個人情報を収集できる機能を持つものがあります。ご使用の「ソフトウェア・オファリング」が、これらの Cookie およびそれに類するテクノロジーを通じてお客様による個人情報の収集を可能にする場合、以下の具体的事項を確認ください。

このソフトウェア・オファリングは、展開される構成に応じて、セッション管理の目的のために、それぞれのお客様のユーザー名と IP アドレスを、セッション Cookie を使用して収集する場合があります。これらの Cookie は無効にできますが、その場合、これらを有効にした場合の機能を活用することはできません。

この「ソフトウェア・オファリング」が Cookie およびさまざまなテクノロジーを使用してエンド・ユーザーから個人を特定できる情報を収集する機能を提供する場合、お客様は、このような情報を収集するにあたって適用される法律、ガイドライン等を遵守する必要があります。これには、エンドユーザーへの通知や同意の要求も含まれますがそれらには限られません。

このような目的での Cookie を含む様々なテクノロジーの使用の詳細については、『[IBM プライバシー・ステートメント](https://www.ibm.com/jp-ja/privacy)』（<https://www.ibm.com/jp-ja/privacy>）、およびセクション『クッキー、ウェブ・ビーコン、

その他のテクノロジー』の『[IBM オンライン・プライバシー・ステートメント](https://www.ibm.com/jp-ja/privacy/details)』(https://www.ibm.com/jp-ja/privacy/details) を参照してください。

プログラミング・インターフェース 情報

この「ハードウェア管理コンソールの管理」資料には、プログラムを作成するユーザーが IBM ハードウェア管理コンソールのバージョン 9 リリース 2 保守レベル 950 のサービスを取得するためのプログラミング・インターフェースについて記載されています。

商標

IBM、IBM ロゴおよび [ibm.com](https://www.ibm.com)® は、世界の多くの国で登録された International Business Machines Corp. の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、Web 上で「[Copyright and trademark information](#)」をご覧ください。

登録商標 Linux は、世界中で商標の所有者である Linux Torvalds の独占的ライセンスである Linux Foundation のサブライセンスに従って使用されています。

Microsoft は、Microsoft Corporation の米国およびその他の国における商標です。

Java およびすべての Java 関連の商標およびロゴは Oracle やその関連会社の米国およびその他の国における商標または登録商標です。

使用条件

これらの資料は、以下の条件に同意していただける場合に限りご使用いただけます。

適用可能性: これらの条件は、IBM Web サイトのすべてのご利用条件に追加されるものです。

個人使用: これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、非商業的な個人による使用目的に限り複製することができます。ただし、IBM の明示的な承諾を得ずに、これらの資料またはその一部について、二次的著作物を作成したり、配布 (頒布、送信を含む) または表示 (上映を含む) することはできません。

商業的使用: これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、お客様の企業内に限り、複製、配布、および表示することができます。ただし、IBM の明示的な承諾を得ずにこれらの資料の二次的著作物を作成したり、お客様の企業外で資料またはその一部を複製、配布、または表示したりすることはできません。

権利: ここで明示的に許可されているもの以外に、資料や資料内に含まれる情報、データ、ソフトウェア、またはその他の知的所有権に対するいかなる許可、ライセンス、または権利を明示的にも黙示的にも付与するものではありません。

資料の使用が IBM の利益を損なうと判断された場合や、上記の条件が適切に守られていないと判断された場合、IBM はいつでも自らの判断により、ここで与えた許可を撤回できるものとさせていただきます。

お客様がこの情報をダウンロード、輸出、または再輸出する際には、米国のすべての輸出入 関連法規を含む、すべての関連法規を遵守するものとします。

IBM は、これらの資料の内容についていかなる保証もしません。これらの資料は、特定物として現存するままの状態 で提供され、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されます。

