ポリシーとプロファイルの管理

この章は、次の内容で構成されています。

クレデンシャル ポリシー

ポリシーは、システムまたはネットワーク リソースへのアクセスを制御するルールのセットから成ります。クレデンシャル ポリシーは、ユーザ アカウントのパスワードの要件とアカウント ロックアウトを定義します。ユーザ アカウントに割り当てられたクレデンシャル ポリシーは、Cisco IMC Supervisor での認証プロセスを制御します。クレデンシャル ポリシーを追加した後、新しいポリシーをクレデンシャル タイプのデフォルトのポリシーとして割り当てるか、または個々のアプリケーションに割り当てることができます。

[Credential Policies] ページには、次の詳細が表示されます。

フィールド	説明
Policy Name	ポリシーのユーザ定義名。
Description	ポリシーのユーザ定義の簡単な説明。
Username	シスコ ユーザ名。
Protocol	ポリシーが準拠するプロトコル。
Port	ポリシーのポート。

このページから、ポリシーの追加、編集、削除など、さまざまなタスクを実行できます。クレデンシャル ポリシーの作成の詳細については、クレデンシャル ポリシーの作成, （2 ページ） を参照してください。

クレデンシャル ポリシーの作成

クレデンシャル ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 メニュー バーで、[Policies] > [Manage Policies] > [Credential Policies] を選択します。

ステップ 2 [Add] をクリックします。

ステップ 3 [Add Credential Policy] ダイアログボックスで、次のフィールドに値を入力します。

フィールド	説明
[Policy Name] フィールド	ポリシーの記述名。
[Description] フィールド	（オプション）ポリシーの説明。
[User Name] フィールド	Cisco IMC ユーザ名またはラックマウント サーバのユーザ名。
[Password] フィールド	Cisco IMC パスワードまたはラックマウント サーバのパスワード。
[Protocol] ドロップダウン リスト	ドロップダウン リストからプロトコルを選択します。
[Port] フィールド	ポリシーのポート番号を入力します。

ステップ 4 [Submit] をクリックします。

ステップ 5 確認ダイアログボックスで、[OK] をクリックします。
作成したクレデンシャル ポリシーのサーバ マッピングの編集、複製、削除、表示、適用、確認ができます。

ハードウェア ポリシー

ポリシーは、Cisco IMC でのさまざまな属性設定を定義するための主要なメカニズムです。ポリシーは、複数のサーバにわたって設定の一貫性と反復可能性を確保するうえで役立ちます。包括

的なポリシー セットを定義して使用すると、多数のサーバに類似する設定を適用できるので、一貫性、制御、予測可能性、自動化が促進されます。

使用例：自身が管理者である場合、適切なネットワーキング、BIOS、RAID 設定などの必要な設定を含んだ「ゴールデン サーバ」が特定できている場合があります。これらの設定を、ポリシーに準拠していない他のサーバ全体に複製することができます。今後、新しいサーバの追加が必要になる場合や、設定済みサーバを展開する場合に備えて、Cisco IMC 内にこの設定を保持することができます。また、同じ内容を適用する前に、その設定をオンザフライで変更することも可能です。たとえば、コンポーネントに更新が必要となったり、NTP IP アドレス、ボー レートなどが必要となる場合があります。「ゴールデン サーバ」での設定を失念していた場合や、他のサーバへの適用前にその内容を確認したい場合もあります。

個々のポリシーは 1 つずつ処理されます。プロファイルにバンドルされているポリシーはマルチスレッド化されており、一連のプロセスを同時に開始するのに役立ちます。

Cisco IMC Supervisor でハードウェア ポリシーを使用する方法を次のワークフローに示します。

1. BIOS ポリシー、NTP ポリシーなどのハードウェア ポリシーを作成します。次のいずれかの方法でポリシーを作成できます。
   a. 新しいポリシーを作成します。さまざまなポリシー タイプ、および新しいポリシーの作成方法の詳細については、ハードウェア ポリシーの作成, （3 ページ）を参照してください。
   b. サーバ上の既存の設定からポリシーを作成します。サーバ上の既存の設定からポリシーを作成する方法の詳細については、既存の設定からのポリシーの作成, （27 ページ）を参照してください。
2. サーバでポリシーを適用します。ポリシーの適用方法の詳細については、ハードウェア ポリシーの適用, （28 ページ）を参照してください。
3. ポリシーで、必要に応じて次のオプション作業を実行します。
   a. Edit
   b. Delete
   c. Clone
   d. また、特定のポリシーにマップされるサーバのリストを表示できます。これらのタスクの実行方法の詳細については、ハードウェア ポリシーでの一般タスク, （29 ページ）を参照してください。
   e. さまざまなポリシーを作成して、それらをプロファイルにグループ化した後、プロファイルをサーバに適用できます。プロファイルの適用方法の詳細については、ハードウェア プロファイルの適用, （33 ページ）を参照してください。

ハードウェア ポリシーの作成

ハードウェア ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 メニュー バーで、[Policies] > [Manage Policies and Profiles] を選択します。

ステップ 2 [Hardware Policies] タブを選択します。

ステップ 3 [Add] をクリックします。

ステップ 4 [Add Policy] ダイアログボックスで、ドロップダウン リストからポリシー タイプを選択します。ポリシー タイプに基づくポリシーの作成の詳細については、以下の表に示されているポリシー タイプを選んでください。これらのポリシーの設定に必要なさまざまなプロパティは、『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』に記載されています。各ポリシー タイプごとに、このマニュアル内の各セクションがリストされています。

ポリシー タイプ	『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』内のセクション
BIOS ポリシー, （5 ページ）	*BIOS* の設定
ディスク グループ ポリシー, （6 ページ）	ストレージ アダプタの管理
FlexFlash ポリシー, （7 ページ）	*Flexible Flash* コントローラの管理
IPMI Over LAN ポリシー, （11 ページ）	*IPMI* の設定
LDAP ポリシー, （12 ページ）	*LDAP* サーバの設定
レガシー ブート順序ポリシー, （13 ページ）	サーバのブート順
ネットワーク構成ポリシー, （14 ページ）	ネットワーク関連の設定
ネットワーク セキュリティ ポリシー, （16 ページ）	ネットワーク セキュリティの設定
NTP ポリシー, （17 ページ）	ネットワーク タイム プロトコル設定の設定
高精度のブート順序ポリシー, （18 ページ）	高精度ブート順の設定
RAID ポリシー, （19 ページ）	ストレージ アダプタの管理
Serial over LAN ポリシー, （20 ページ）	*Serial over LAN* の設定
SNMP ポリシー, （21 ページ）	*SNMP* の設定
SSH ポリシー, （22 ページ）	*SSH* の設定
ユーザ ポリシー, （23 ページ）	ローカル ユーザの設定

ポリシー タイプ	『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』内のセクション
VIC アダプタ ポリシー, （25 ページ）	*VIC* アダプタのプロパティの表示
仮想 KVM ポリシー, （24 ページ）	仮想 *KVM* の設定
vMedia ポリシー, （26 ページ）	仮想メディアの設定

次の作業

サーバにポリシーを適用します。ポリシーの適用方法の詳細については、ハードウェア ポリシーの適用, （28 ページ）を参照してください。

BIOS ポリシー

BIOS ポリシーは、サーバの BIOS 設定を自動化します。1 つのサーバまたはサーバ セットのニーズに適合する特定の BIOS 設定のグループを含む、1 つ以上の BIOS ポリシーを作成することができます。あるサーバの BIOS ポリシーを指定しない場合、BIOS 設定は現状のまま、つまり、デフォルト値のセット（新品のベア メタル サーバの場合）、あるいは Cisco IMC を使って設定された値のセットになります。BIOS ポリシーを指定した場合、サーバで設定済みの値が、ポリシーで指定された値に置き換わります。

さまざまな BIOS プロパティの設定の詳細については、『*Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide*』の「*Configuring BIOS Settings*」の項を参照してください。

BIOS ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 [Hardware Policies] ページで、[Add] をクリックします。
このページに移動する方法の詳細については、ハードウェア ポリシーの作成, （3 ページ）を参照してください。

ステップ 2 [Add] ダイアログボックスで、ドロップダウン リストから [BIOS Policy] を選択して [Submit] をクリックします。

ステップ 3 [Policy Name] フィールドに名前を入力して、[Next] をクリックします。
また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[Server Details] ダイアログボックスが表示されます。このダイアログボックスでのタスクの実行については、既存の設定からのポリシーの作成, （27 ページ）を参照してください。

（注） Cisco IMC Supervisor のプロパティまたは属性のうち、特定の Cisco IMC バージョンを実行するサーバに該当しないものがある場合、それらは適用できません。プロパティが Cisco IMC サーバで利用可能でない場合、そのプロパティ フィールドには [Platform-Default] として表示されます。

ステップ 4 [Main] ダイアログボックスで、主要な BIOS プロパティ（[Boot Option Retry]、[Post Error Pause]、[TPM Support] ドロップダウン リストなど）の値を選択します。

ステップ 5 [Advanced] ダイアログボックスで、BIOS のプロパティ値をドロップダウン リストから選択して [Next] をクリックします。

ステップ 6 [Server Management] ダイアログボックスで、サーバのプロパティ値をドロップダウン リストから選択して [Submit] をクリックします。

ステップ 7 [Submit Result] ダイアログボックスで、[OK] をクリックします。

ディスク グループ ポリシー

ディスク グループ ポリシーを使用すると、仮想ドライブに使われる物理ディスクを選択することができ、特定の仮想ドライブに関連するさまざまな属性の設定もできます。仮想ドライブの作成に使用される物理ディスクのグループは、ディスク グループと呼ばれます。

ディスク グループ ポリシーは、ディスク グループの作成方法と設定方法を定義します。このポリシーは、仮想ドライブに使用される RAID レベルを指定します。1 つのディスク グループ ポリシーを使用して、複数のディスク グループを管理できます。1 つのディスク グループ ポリシーを複数の仮想ドライブに関連付けることができます。その場合、それらの仮想ドライブは同じ仮想ドライブ グループ スペースを共有します。1 つの RAID ポリシー内の複数の異なる仮想ドライブに関連付けられるディスク グループ ポリシーが使用するいずれかの物理ディスクを、別のディスク グループ ポリシーで繰り返し使用することはありません。RAID ポリシーの詳細については、RAID ポリシー, （19 ページ）を参照してください。

さまざまなディスク グループ プロパティの設定の詳細については、『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』の「*Managing Storage Adapters*」の項を参照してください。

ディスク グループ ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 [Hardware Policies] ページで、[Add] をクリックします。
このページに移動する方法の詳細については、ハードウェア ポリシーの作成, （3 ページ）を参照してください。

ステップ 2 [Add] ダイアログボックスで、ドロップダウン リストから [Disk Group Policy] を選択して [Submit] をクリックします。

ステップ 3 [Policy Name] フィールドに名前を入力して、[Next] をクリックします。

ステップ 4 [Virtual Drive Configuration] ダイアログボックスで、仮想ドライブ プロパティを選択して [Next] をクリックします。

ステップ 5 [Local Disk Configuration] ダイアログボックスで、[+] をクリックしてローカル ディスク設定を参照するエントリを追加し、[Submit] をクリックします。

ステップ 6 [Submit Result] ダイアログボックスで、[OK] をクリックします。

ステップ 7 [Main] ダイアログボックスで [Submit] をクリックします。

ステップ 8 [Submit Result] ダイアログボックスで、[OK] をクリックします。

（注）
- サーバの現在の設定からディスク グループ ポリシーを作成することはできません。
- サーバの現在の設定から RAID ポリシーが作成されるときに、ディスク グループ ポリシーもまたサーバ設定から自動的に作成されます。

FlexFlash ポリシー

FlexFlash ポリシーを使用して、SD カードを設定して有効にすることができます。

さまざまなプロパティの設定の詳細については、『*Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide*』の「*Managing the Flexible Flash Controller*」の項を参照してください。

（注） FlexFlash をサポートする最小の Cisco Integrated Management Controller のファームウェア バージョンは 2.0(2c) です。

FlexFlash ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 [Hardware Policies] ページで、[Add] をクリックします。
このページに移動する方法の詳細については、ハードウェア ポリシーの作成, （3 ページ）を参照してください。

ステップ 2 [Add] ダイアログボックスで、ドロップダウン リストから [FlexFlash Policy] を選択して [Submit] をクリックします。

ステップ 3 [Policy Name] フィールドに名前を入力して、[Next] をクリックします。
また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[Server Details] ダイアログボックスが表示されます。このダイアログボックスでのタスクの実行については、既存の設定からのポリシーの作成, （27 ページ）を参照してください。

ステップ 4 [Configure Cards] ダイアログボックスで、次のフィールドに値を入力します。

フィールド	説明
[Firmware Mode] ペイン	次のファームウェア動作モードのいずれかを選択します。 • [Mirror Mode]：このモードはミラー設定で、C220 M4 および C240 M4 サーバでのみ使用できます。 • [Util Mode]：このモードでは、4 つのパーティションを持つ 1 つのカードと、単一パーティションを持つ 1 つのカードが作成されます。このモードを使用できるのは C220 M4 および C240 M4 サーバのみです。 • [Not Applicable]：ファームウェアの動作モードが選択されません。[Not Applicable] を選択した場合はステップ 5 に進みます。このモードは、C220 M3、C240 M3、C22、C24、C460 M4 サーバでのみ使用できます。
[Partition Name] フィールド	パーティションの名前。
[Non Util Card Partition Name] フィールド	2 枚目のカードの単一パーティションに割り当てる名前（存在する場合）。 （注） このオプションは、util モードの場合にのみ使用できます。
[Select Primary Card]（ミラー モードで使用可能）または [Select Util Card]（Util モードで使用可能）ドロップダウン リスト	SD カードが配置されているスロット [Slot 1] または [Slot 2] を選択するか、または SD カードがサーバに 1 枚しかない場合は [None] を選択します。 （注） [None] は [Select Util Card] オプションでのみ使用できます。
[Auto Sync] チェックボックス	選択したスロットで使用可能な SD カードを自動的に同期します。 （注） このオプションは、ミラー モードの場合にのみ使用できます。

フィールド	説明
[Slot-1 Read Error Threshold] フィールド	Cisco FlexFlash カードのスロット 1 へのアクセス中に許可される読み取りエラーの数。読み取りエラーの数がカード上のこのしきい値を超えると、カードが正常でないとマークされます。 読み取りエラーのしきい値を指定するには、1 ～ 255 の整数を入力します。検出されたエラー数に関係なく、カードがディセーブルにならないように指定するには、0（ゼロ）を入力します。
[Slot-1 Write Error Threshold] フィールド	Cisco FlexFlash カードのスロット 1 へのアクセス中に許可される書き込みエラーの数。書き込みエラーの数がカード上のこのしきい値を超えると、カードが正常でないとマークされます。 書き込みエラーのしきい値を指定するには、1 ～ 255 の整数を入力します。検出されたエラー数に関係なく、カードがディセーブルにならないように指定するには、0（ゼロ）を入力します。
[Slot-2 Read Error Threshold] フィールド	Cisco FlexFlash カードのスロット 2 へのアクセス中に許可される読み取りエラーの数。読み取りエラーの数がカード上のこのしきい値を超えると、カードが正常でないとマークされます。 読み取りエラーのしきい値を指定するには、1 ～ 255 の整数を入力します。検出されたエラー数に関係なく、カードがディセーブルにならないように指定するには、0（ゼロ）を入力します。 （注） このオプションは、util モードの場合にのみ使用できます。ミラー モードの場合は、スロット 1 の読み取り/書き込みしきい値がスロット 2 にも適用されます。

フィールド	説明
[Slot-2 Write Error Threshold] フィールド	Cisco FlexFlash カードのスロット 2 へのアクセス中に許可される書き込みエラーの数。書き込みエラーの数がカード上のこのしきい値を超えると、カードが正常でないとマークされます。 書き込みエラーのしきい値を指定するには、1 ～ 255 の整数を入力します。検出されたエラー数に関係なく、カードがディセーブルにならないように指定するには、0（ゼロ）を入力します。 （注） このオプションは、util モードの場合にのみ使用できます。ミラー モードの場合は、スロット 1 の読み取り/書き込みしきい値がスロット 2 にも適用されます。

ステップ 5 ステップ 4 の [Details] ペインで [Not Applicable] を選択した場合は、次のフィールドに値を入力します。

フィールド	説明
[Virtual Drive Enable] ドロップダウン リスト	USB 形式のドライブとして、サーバに対して使用可能にできる仮想ドライブ。
[RAID Primary Member] ドロップダウン リスト	プライマリ RAID メンバが存在するスロット。
[RAID Secondary Role] ドロップダウン リスト	セカンダリ RAID の役割です。
[I/O Read Error Threshold] フィールド	Cisco FlexFlash カードへのアクセス中に許可される読み取りエラーの数。読み取りエラーの数がカード上のこのしきい値を超えると、カードが正常でないとマークされます。 読み取りエラーのしきい値を指定するには、1 ～ 255 の整数を入力します。検出されたエラー数に関係なく、カードがディセーブルにならないように指定するには、0（ゼロ）を入力します。

フィールド	説明
[I/O Write Error Threshold] フィールド	Cisco FlexFlash カードへのアクセス中に許可される書き込みエラーの数。書き込みエラーの数がカード上のこのしきい値を超えると、カードが正常でないとマークされます。 Cisco FlexFlash カードへのアクセス中に許可される書き込みエラーの数。書き込みエラーの数がカード上のこのしきい値を超えると、カードが正常でないとマークされます。
[Clear Errors] チェックボックス	オンにした場合、[Submit] をクリックすると、読み取り/書き込みエラーがクリアされます。

ステップ 6 [Submit] をクリックします。

ステップ 7 [Submit Result] ダイアログボックスで、[OK] をクリックします。
また、[Hardware Policies] テーブルから既存の FlexFlash ポリシーを選択し、ユーザ インターフェイスで該当するオプションを選択することで、適用ステータスの削除、編集、複製、適用、表示が行えます。

（注） FlexFlash ポリシーの適用は、次のように 2 つのステップからなるプロセスです。

1. サーバの設定がデフォルトに設定されます。
2. ポリシーの新しい設定が適用されます。したがって、この手順で失敗すると、ポリシーを適用する前に既存の設定が失われます。

IPMI Over LAN ポリシー

インテリジェント プラットフォーム管理インターフェイス（IPMI）では、サーバ プラットフォームに組み込まれているサービス プロセッサとのインターフェイスのためのプロトコルを定義しています。このサービス プロセッサはベースボード管理コントローラ（BMC）と呼ばれ、サーバのマザーボードに存在します。BMC は、メイン プロセッサおよびボード上の他の要素に、簡単なシリアル バスを使用してリンクします。Cisco IMC を IPMI メッセージで管理するには、IPMI over LAN ポリシーを設定します。

さまざまなプロパティの設定の詳細については、『*Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide*』の「*Configuring IPMI*」の項を参照してください。

IPMI Over LAN ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 [Hardware Policies] ページで、[Add] をクリックします。
このページに移動する方法の詳細については、ハードウェア ポリシーの作成, （3 ページ）を参照してください。

ステップ 2 [Add] ダイアログボックスで、ドロップダウン リストから [IPMI Over LAN Policy] を選択して [Submit] をクリックします。

ステップ 3 [Policy Name] フィールドに名前を入力して、[Next] をクリックします。
また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[Server Details] ダイアログボックスが表示されます。このダイアログボックスでのタスクの実行については、既存の設定からのポリシーの作成, （27 ページ）を参照してください。

ステップ 4 [Main] ダイアログボックスで、次のフィールドに値を入力します。

オプション	説明
[Enable IPMI Over LAN]	IPMI プロパティを設定するには、このチェックボックスをオンにします。
[Privilege Level Limit]	ドロップダウン リストから特権レベルを選択します。
Encryption Key	このフィールドにキーを入力します。

（注） 暗号キーに含まれる 16 進数文字の数は偶数でなければならず、長さの合計が 40 文字を超えてはなりません。40 文字未満が指定されている場合、キーの長さが 40 になるまでゼロが埋め込まれます。

ステップ 5 [Submit] をクリックします。

ステップ 6 [Submit Result] ダイアログボックスで、[OK] をクリックします。

LDAP ポリシー

Cisco C シリーズと E シリーズのサーバは LDAP をサポートし、Cisco IMC Supervisor は LDAP ポリシーを使用してサーバでの LDAP 設定をサポートします。1 つのサーバまたはサーバ セットのニーズに適合する特定の LDAP 設定のグループを含む、1 つ以上の LDAP ポリシーを作成することができます。

さまざまな LDAP プロパティの設定の詳細については、『*Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide*』の「*Configuring LDAP Server*」の項を参照してください。

LDAP ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 [Hardware Policies] ページで、[Add] をクリックします。
このページに移動する方法の詳細については、ハードウェア ポリシーの作成, （3 ページ）を参照してください。

ステップ 2 [Add] ダイアログボックスで、ドロップダウン リストから [LDAP Policy] を選択して [Submit] をクリックします。

ステップ 3 [Policy Name] フィールドに名前を入力して、[Next] をクリックします。
また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[Server Details] ダイアログボックスが表示されます。このダイアログボックスでのタスクの実行については、既存の設定からのポリシーの作成, （27 ページ）を参照してください。

ステップ 4 [Main] ダイアログボックスで、LDAP プロパティを入力します。

ステップ 5 [Next] をクリックします。

ステップ 6 [LDAP Servers] ダイアログボックスで、LDAP サーバの詳細を入力します。

ステップ 7 [Next] をクリックします。

ステップ 8 [Group Authorization] ダイアログボックスでグループ認証の詳細を入力し、[+] をクリックして LDAP グループ エントリをテーブルに追加します。

ステップ 9 [Add Entry to LDAP Groups] ダイアログボックスで、グループの詳細を入力します。

ステップ 10 [Submit] をクリックします。

ステップ 11 [Submit Result] ダイアログボックスで、[OK] をクリックします。

ステップ 12 [Group Authorization] ダイアログボックスで [Submit] をクリックします。

ステップ 13 [Submit Result] ダイアログボックスで、[OK] をクリックします。

（注）
- 設定済みの LDAP ロール グループがサーバに存在する場合、それらはすべて削除され、ポリシーで設定したロール グループに置き換わります。ポリシーにロール グループをまだ追加していない場合、サーバ上の既存のロール グループは削除されますが、置換されません。
- [Nested Group Search Depth] は、Cisco IMC バージョン 2.0(4c) 以上にのみ適用できます。2.0(4c) より前のバージョンの Cisco IMC を実行しているサーバには、ポリシーを使ってこの値を適用することはできません。

レガシー ブート順序ポリシー

レガシー ブート順序ポリシーは、ブート順序の設定を自動化します。1 つのサーバまたはサーバ セットのニーズに適合する特定のブート順序設定のグループを含む、1 つ以上のレガシー ブート順序ポリシーを作成することができます。Cisco IMC Supervisor を使用して、使用可能なブート デバイス タイプからサーバがブートを試行する順序を設定できます。また、デバイスの線形順序付

けを可能にする高精度ブート順序を設定することもできます。高精度ブート順序の詳細については、 高精度のブート順序ポリシー, （18 ページ）を参照してください。

さまざまなサーバ ブート順序プロパティの設定の詳細については、『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』の「*Server Boot Order*」の項を参照してください。

レガシー ブート順序ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 [Hardware Policies] ページで、[Add] をクリックします。
このページに移動する方法の詳細については、ハードウェア ポリシーの作成, （3 ページ）を参照してください。

ステップ 2 [Add] ダイアログボックスで、ドロップダウン リストから [Legacy Boot Order Policy] を選択して [Submit] をクリックします。

ステップ 3 [Policy Name] フィールドに名前を入力して、[Next] をクリックします。
また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[Server Details] ダイアログボックスが表示されます。このダイアログボックスでのタスクの実行については、既存の設定からのポリシーの作成, （27 ページ）を参照してください。

ステップ 4 [Main] ダイアログボックスで [+] をクリックして、ドロップダウン リストからデバイス タイプを選択します。追加したデバイスがテーブルにリストされます。
[Select Devices] テーブルで、既存のデバイスを選択して [x] をクリックするとデバイスが削除されます。エントリの順序を変更するには、上/下矢印アイコンを使用します。テーブルのエントリの順序により、ブート順序が決まります。

同じデバイス タイプをさらに追加することはできません。

ステップ 5 [Add Entry to Select Devices] ダイアログボックスで [Submit] をクリックします。

ステップ 6 [Submit Result] ダイアログボックスで、[OK] をクリックします。

ステップ 7 [Main] ダイアログボックスで [Submit] をクリックします。

ステップ 8 [Submit Result] ダイアログボックスで、[OK] をクリックします。

（注） このポリシーは、2.0 より前のバージョンの Cisco IMC にのみ適用できます。それ以降のバージョンの Cisco IMC を実行するサーバに対してポリシーが適用された場合、エラー メッセージが表示されます。代わりに高精度ブート順序ポリシーを使用してください。

ネットワーク構成ポリシー

Cisco IMC Supervisor では、ダイナミック DNS、IPv4、IPv6、VLAN などの各種プロパティを使用して、ネットワーク構成ポリシーを作成できます。

さまざまなネットワーク構成プロパティの設定の詳細については、『*Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide*』の「*Configuring Network-Related Settings*」の項を参照してください。

ネットワーク構成ポリシーを作成するには、次の手順を実行します。

はじめる前に

手順

ステップ 1 [Hardware Policies] ページで、[Add] をクリックします。このページに移動する方法の詳細については、ハードウェア ポリシーの作成, （3 ページ）を参照してください。

ステップ 2 [Add] ダイアログボックスで、ドロップダウン リストから [Network Configuration Policy] を選択して [Submit] をクリックします。

ステップ 3 [Policy Name] フィールドに名前を入力して、[Next] をクリックします。また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[Server Details] ダイアログボックスが表示されます。このダイアログボックスでのタスクの実行については、既存の設定からのポリシーの作成, （27 ページ）を参照してください。

ステップ 4 [Main] ダイアログボックスで、次のフィールドに値を入力します。

フィールド	説明
共通のプロパティ	
[Use Dynamic DNS] チェックボックス	ダイナミック DNS は、Cisco IMC Supervisor から DNS サーバのリソース レコードを追加または更新するために使用されます。
IPv4 プロパティ	
[Obtain DNS Server Addresses from DHCP] チェックボックス	オンにすると、Cisco IMC Supervisor は DNS サーバ アドレスを DHCP から取得します。
[Preferred DNS Server] フィールド	プライマリ DNS サーバの IP アドレス。
[Alternate DNS Server] フィールド	セカンダリ DNS サーバの IP アドレス。
IPv6 プロパティ	
[Obtain DNS Server Addresses from DHCP] チェックボックス	オンにすると、Cisco IMC Supervisor は DNS サーバ アドレスを DHCP から取得します。
[Preferred DNS Server] フィールド	プライマリ DNS サーバの IP アドレス。
[Alternate DNS Server] フィールド	セカンダリ DNS サーバの IP アドレス。

フィールド	説明
VLAN プロパティ	
[Enable VLAN] チェックボックス	オンにすると、仮想 LAN に接続されます。

ステップ 5 [Submit] をクリックします。

ステップ 6 [Submit Result] ダイアログボックスで、[OK] をクリックします。

ネットワーク セキュリティ ポリシー

Cisco IMC Supervisor は、ネットワーク セキュリティとして IP ブロッキングを使用します。IP ブロッキングは、サーバまたは Web サイトと、特定の IP アドレスまたはアドレス範囲との間の接続を防ぎます。IP ブロッキングは、これらのコンピュータから Web サイト、メール サーバ、またはその他のインターネット サーバへの不要な接続を効果的に禁止します。1 つのサーバまたはサーバ セットのニーズに適合する特定の IP プロパティのグループを含む、1 つ以上のネットワーク セキュリティ ポリシーを作成できます。

さまざまなネットワーク セキュリティ プロパティの設定の詳細については、『*Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide*』の「*Network Security Configuration*」の項を参照してください。

ネットワーク セキュリティ ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 [Hardware Policies] ページで、[Add] をクリックします。
このページに移動する方法の詳細については、ハードウェア ポリシーの作成, （3 ページ）を参照してください。

ステップ 2 [Add] ダイアログボックスで、ドロップダウン リストから [Network Security] を選択して [Submit] をクリックします。

ステップ 3 [Policy Name] フィールドに名前を入力して、[Next] をクリックします。
また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[Server Details] ダイアログボックスが表示されます。このダイアログボックスでのタスクの実行については、既存の設定からのポリシーの作成, （27 ページ）を参照してください。

ステップ 4 [Main] ダイアログボックスで、IP をブロックするために [Enable IP Blocking] チェックボックスをオンにし、IP ブロック プロパティを設定するために属性を入力します。

ステップ 5 [Submit] をクリックします。

ステップ 6 [Submit Result] ダイアログボックスで、[OK] をクリックします。

NTP ポリシー

NTP サービスを使用すると、NTP サーバとの間で時刻を同期するよう、Cisco IMC Supervisor によって管理されるサーバを設定できます。デフォルトでは、Cisco IMC Supervisor では NTP サーバが動作しません。NTP サービスを有効にして設定する必要があります。その際、NTP サーバとして動作する少なくとも 1 台、最大 4 台のサーバの IP/DNS アドレスを指定します。NTP サービスを有効にすると、Cisco IMC Supervisor は、管理対象サーバと設定済み NTP サーバとの間で時刻を同期します。

さまざまな NTP プロパティの設定の詳細については、『*Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide*』の「*Configuring Network Time Protocol Settings*」の項を参照してください。

NTP ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 [Hardware Policies] ページで、[Add] をクリックします。
このページに移動する方法の詳細については、ハードウェア ポリシーの作成, （3 ページ）を参照してください。

ステップ 2 [Add] ダイアログボックスで、ドロップダウン リストから [NTP Policy] を選択して [Submit] をクリックします。

ステップ 3 [Policy Name] フィールドに名前を入力して、[Next] をクリックします。
また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[Server Details] ダイアログボックスが表示されます。このダイアログボックスでのタスクの実行については、既存の設定からのポリシーの作成, （27 ページ）を参照してください。

ステップ 4 [Main] ダイアログボックスで、[Enable NTP] チェックボックスをオンにして代替サーバを有効にし、NTP サーバを 4 つまで指定します。

ステップ 5 [Submit] をクリックします。

ステップ 6 [Submit Result] ダイアログボックスで、[OK] をクリックします。

（注） このポリシーは、E シリーズ サーバ モデルには適用できません。

高精度のブート順序ポリシー

高精度のブート順序を設定すると、デバイスの線形順序付けが可能になります。Cisco IMC Supervisor では、ブート順序とブート モードの変更、各デバイス タイプの下への複数のデバイスの追加、ブート順序の並び替え、各デバイス タイプのパラメータの設定ができます。
さまざまなブート順序プロパティの設定の詳細については、『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』の「*Configuring the Precision Boot Order*」の項を参照してください。

このポリシーは、Cisco IMC バージョン 2.x 以上を実行しているサーバ用に作成できます。2.x より前のバージョンを実行しているサーバの場合、代わりにレガシー ブート順序ポリシーを設定する必要があります。

高精度ブート順序ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 [Hardware Policies] ページで、[Add] をクリックします。
このページに移動する方法の詳細については、ハードウェア ポリシーの作成, （3 ページ）を参照してください。

ステップ 2 [Add] ダイアログボックスで、ドロップダウン リストから [Precision Boot Order Policy] を選択して [Submit] をクリックします。

ステップ 3 [Policy Name] フィールドに名前を入力して、[Next] をクリックします。
また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[Server Details] ダイアログボックスが表示されます。このダイアログボックスでのタスクの実行については、既存の設定からのポリシーの作成, （27 ページ）を参照してください。

ステップ 4 [Main] ダイアログボックスで、[UEFI Secure Boot] チェックボックスをオンにするか、[Configure Boot Mode] ドロップダウン リストからブート モードを選択します。

ステップ 5 [+] をクリックして、デバイスの詳細を選択または入力します。追加したデバイスがテーブルにリストされます。
また、[Select Devices] テーブルで既存のデバイスを選択し、[x] をクリックして削除したり、編集アイコンをクリックしてデバイスを編集したりすることもできます。エントリの順序を変更するには、上/下矢印アイコンを使用します。テーブルのエントリの順序により、ブート順序が決まります。

ステップ 6 [Add Entry to Select Devices] ダイアログボックスで [Submit] をクリックします。

ステップ 7 [Submit Result] ダイアログボックスで、[OK] をクリックします。

ステップ 8 [Main] ダイアログボックスで [Submit] をクリックします。

ステップ 9 [Submit Result] ダイアログボックスで、[OK] をクリックします。

RAID ポリシー

RAIDポリシーを使用すると、サーバ上に仮想ドライブを作成できます。仮想ドライブのストレージ容量も設定できます。RAIDポリシー内のそれぞれの仮想ドライブは、1つのディスク グループ ポリシーに関連付けられます。ディスク グループ ポリシーを使用すると、特定の仮想ドライブに使われるディスクを選択し、設定することができます。

RAID ポリシーは、以下の環境でのみサポートされます。

- RAID 設定をサポートするストレージ コントローラ。
- Cisco IMC ファームウェア バージョン 2.0(4c) 以上。
- 単一のストレージ コントローラを含むサーバ。複数のストレージ コントローラを含むサーバでは、RAID ポリシーは最初のスロットのストレージ コントローラにのみ適用されます。

さまざまなプロパティの設定の詳細については、『*Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide*』の「*Managing Storage Adapters*」の項を参照してください。

RAID ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 [Hardware Policies] ページで、[Add] をクリックします。
このページに移動する方法の詳細については、ハードウェア ポリシーの作成, （3 ページ）を参照してください。

ステップ 2 [Add] ダイアログボックスで、ドロップダウン リストから [RAID Policy] を選択して [Submit] をクリックします。

ステップ 3 [Policy Name] フィールドに名前を入力して、[Next] をクリックします。
また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[Server Details] ダイアログボックスが表示されます。このダイアログボックスでのタスクの実行については、既存の設定からのポリシーの作成, （27 ページ）を参照してください。

ステップ 4 [Main] ダイアログボックスで [+] をクリックすると、サーバ上に設定する仮想ドライブを [Virtual Drives] リストに追加できます。

ステップ 5 [Add Entry to Virtual Drives] ダイアログボックスで、仮想ドライブの詳細を入力または選択します。ドロップダウン リストから既存のディスク グループ ポリシーを選択して編集するか、新しいディスク グループ ポリシーを追加してローカルディスクを指定することができます。ディスク グループ ポリシーを作成するには、ディスク グループ ポリシー, （6 ページ）を参照してください。

（注） 2 つの仮想ドライブが作成されて同じディスク グループ ポリシーに関連付けられた場合、それらは同じ仮想ドライブ グループ スペースを共有します。

ステップ 6 [Add Entry] ダイアログボックスで [Submit] をクリックします。

ステップ 7 [Submit Result] ダイアログボックスで、[OK] をクリックします。

ステップ 8 サーバ上の既存のすべての仮想ドライブを削除するには、[Erase existing Virtual Drives] チェックボックスをオンにします。
このチェックボックスを選択した場合、ポリシーの適用時に、サーバ上の既存のすべての仮想ドライブが削除されます。その結果、既存のデータは消失します。

ステップ 9 残りのディスクを JBOD として設定するには、[Configure remaining disks as JBOD] チェックボックスをオンにします。
このオプションは、JBOD をサポートするストレージ コントローラにのみ適用できます。仮想ドライブやホット スペアに使用されないディスクは、JBOD として設定されます。

ステップ 10 [Main] ダイアログボックスで [Submit] をクリックします。

ステップ 11 [Submit Result] ダイアログボックスで、[OK] をクリックします。

Serial over LAN ポリシー

Serial over LAN を使用すると、管理対象システムのシリアル ポートの入出力を IP 経由でリダイレクトできます。Cisco IMC Supervisor を使用してホスト コンソールに到達するには、サーバで Serial over LAN を設定して使用します。1 つのサーバまたはサーバ セットのニーズに適合する特定の Serial over LAN 属性のグループを含む、1 つ以上の Serial over LAN ポリシーを作成できます。

さまざまな Serial over LAN プロパティの設定の詳細については、『*Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide*』の「*Configuring Serial Over LAN*」の項を参照してください。

Serial over LAN ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 [Hardware Policies] ページで、[Add] をクリックします。
このページに移動する方法の詳細については、ハードウェア ポリシーの作成, （3 ページ）を参照してください。

ステップ 2 [Add] ダイアログボックスで、ドロップダウン リストから [Serial Over LAN Policy] を選択して [Submit] をクリックします。

ステップ 3 [Policy Name] フィールドに名前を入力して、[Next] をクリックします。
また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[Server Details] ダイアログボックスが表示されます。このダイアログボックスでのタスクの実行については、既存の設定からのポリシーの作成, （27 ページ）を参照してください。

ステップ 4 [Main] ダイアログボックスで、[Enable SoL] チェックボックスをオンにして、ドロップダウン リストから [CoM Port] 値と [Baud Rate] 値を選択するか、既存の値を使用します。

ステップ 5 [Submit] をクリックします。

ステップ 6 [Submit Result] ダイアログボックスで、[OK] をクリックします。

SNMP ポリシー

Cisco IMC Supervisor は Simple Network Management Protocol（SNMP）の設定をサポートし、管理対象サーバから SNMP トラップによって障害とアラートの情報を送信するための設定が可能です。

さまざまな SNMP プロパティの設定の詳細については、『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』の「*Configuring SNMP*」の項を参照してください。

SNMP ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 [Hardware Policies] ページで、[Add] をクリックします。
このページに移動する方法の詳細については、ハードウェア ポリシーの作成, （3 ページ）を参照してください。

ステップ 2 [Add] ダイアログボックスで、ドロップダウン リストから [SNMP Policy] を選択して [Submit] をクリックします。

ステップ 3 [Policy Name] フィールドに名前を入力して、[Next] をクリックします。
また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[Server Details] ダイアログボックスが表示されます。このダイアログボックスでのタスクの実行については、既存の設定からのポリシーの作成, （27 ページ）を参照してください。

ステップ 4 [SNMP Users] ダイアログボックスで [+] をクリックして SNMP ユーザを追加し、ユーザの詳細情報を入力します。[+] アイコンを使用して、最大で 15 SNMP ユーザを追加することができます。
既存の SNMP エントリを選択すると、そのエントリを編集またはテーブルから削除できます。

ステップ 5 [Next] をクリックします。

ステップ 6 [SNMP Traps] ダイアログボックスで [+] をクリックして SNMP トラップを追加し、トラップの詳細情報を入力します。[+] アイコンを使用して、最大で 15 個の SNMP トラップを追加することができます。
既存の SNMP エントリを選択すると、そのエントリを編集またはテーブルから削除できます。

ステップ 7 [Next] をクリックします。

ステップ 8 [SNMP Settings] ダイアログボックスで、SNMP プロパティを設定します。

ステップ 9 [Submit] をクリックします。

ステップ 10 [Submit Result] ダイアログボックスで、[OK] をクリックします。

（注）
- サーバで以前に設定されていた既存の [SNMP Users] または [SNMP Traps] が削除され、ポリシーで設定したユーザやトラップに置き換わります。ポリシーにユーザやトラップをまだ追加していない場合は、サーバ上の既存のユーザまたはトラップが削除されますが、置き換わりません。
- 2.x より前のバージョンの Cisco IMC を実行している C シリーズ サーバでは [SNMP Port] を設定できません。チェックボックスを使用して、そのようなサーバは除外する必要があります。
- Cisco IMC バージョン 2.x を実行している E シリーズ サーバでは [SNMP Port] を設定できません。チェックボックスを使用して、そのようなサーバは除外する必要があります。

SSH ポリシー

SSH サーバは、SSH クライアントがセキュアな暗号化された接続を行えるようにします。SSH クライアントは、SSHプロトコルで動作し、デバイスの認証および暗号化を提供するアプリケーションです。1 つのサーバまたはサーバ セットのニーズに適合する特定の SSH プロパティのグループを含む、1 つ以上の SSH ポリシーを作成することができます。

さまざまな SSH プロパティの設定の詳細については、『*Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide*』の「*Configuring SSH*」の項を参照してください。

SSH ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 [Hardware Policies] ページで、[Add] をクリックします。
このページに移動する方法の詳細については、ハードウェア ポリシーの作成, （3 ページ）を参照してください。

ステップ 2 [Add] ダイアログボックスで、ドロップダウン リストから [SSH Policy] を選択して [Submit] をクリックします。

ステップ 3 [Policy Name] フィールドに名前を入力して、[Next] をクリックします。
また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[Server Details] ダイアログボックスが表示されます。このダイアログボックスでのタスクの実行については、既存の設定からのポリシーの作成, （27 ページ）を参照してください。

ステップ 4 [Main] ダイアログボックスで [Enable SSH] チェックボックスをオンにして、SSH プロパティを入力するか、または既存のプロパティを使用します。

ステップ 5 [Submit] をクリックします。

ステップ 6 [Submit Result] ダイアログボックスで、[OK] をクリックします。

ユーザ ポリシー

ユーザ ポリシーは、ローカル ユーザの設定を自動化します。1 つのサーバまたはサーバのグループに設定される必要のあるローカル ユーザ リストを含む、1 つ以上のユーザ ポリシーを作成することができます。

さまざまなプロパティの設定の詳細については、『*Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide*』の「*Configuring Local Users*」の項を参照してください。

ユーザ ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 [Hardware Policies] ページで、[Add] をクリックします。
このページに移動する方法の詳細については、ハードウェア ポリシーの作成, （3 ページ）を参照してください。

ステップ 2 [Add] ダイアログボックスで、ドロップダウン リストから [User Policy] を選択して [Submit] をクリックします。

ステップ 3 [Policy Name] フィールドに名前を入力して、[Next] をクリックします。
また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[Server Details] ダイアログボックスが表示されます。このダイアログボックスでのタスクの実行については、既存の設定からのポリシーの作成, （27 ページ）を参照してください。

ステップ 4 [Main] ダイアログボックスで、サーバに設定する必要があるユーザを [Users] リストに追加できます。

ステップ 5 [+] をクリックして、ユーザを追加します。

ステップ 6 [Add Entry to Users] ダイアログボックスで、次のフィールドに入力します。

フィールド	説明
Username	ユーザの名前をフィールドに入力します。
Role	読み取り専用、管理などのユーザ ロールをドロップダウン リストから選択します。
Enabled	ユーザをアクティブにするには、このチェックボックスをオンにします。

フィールド	説明
New Password	ユーザ名に関連付けられるパスワードを入力します。
Confirm New Password	前のフィールドと同じパスワードを入力します。

ステップ 7 [Submit] をクリックします。

ステップ 8 [Submit Result] ダイアログボックスで、[OK] をクリックします。
また、[Main] ダイアログボックスの [Users] テーブルで既存のユーザを選択し、[Edit] または [Delete] アイコンをクリックしてユーザを編集/削除することもできます。

（注）
- [Users] テーブルの最初のユーザは、管理ユーザです。この管理ユーザを削除することはできませんが、パスワードは変更できます。
- ユーザ ポリシーを適用すると、Cisco IMC Supervisor 内のユーザ エントリが、作成したユーザ エントリに置き換わります。Cisco IMC 内の空白のエントリは Cisco IMC Supervisor のデフォルト ユーザに置き換えられます。デフォルト ユーザ ロールは常に読み取り専用であり、ユーザは無効になっています。
- Cisco IMC Supervisor の管理に使用されるアカウントは、ポリシーのユーザ リストから決して削除しないでください。削除した場合、Cisco IMC Supervisor は管理対象サーバへの接続を失います。

仮想 KVM ポリシー

KVM コンソールは Cisco IMC Supervisor からアクセス可能なインターフェイスであり、サーバへのキーボード、ビデオ、マウス（KVM）の直接接続をエミュレートします。KVM コンソールを使用すると、リモートの場所からサーバに接続できます。1 つのサーバまたはサーバセットのニーズに適合する特定の仮想 KVM プロパティのグループを含む、1 つ以上の KVM ポリシーを作成することができます。

さまざまな KVM プロパティの設定の詳細については、『*Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide*』の「*Configuring the Virtual KVM*」の項を参照してください。

仮想 KVM ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 [Hardware Policies] ページで、[Add] をクリックします。

このページに移動する方法の詳細については、ハードウェア ポリシーの作成, （3 ページ）を参照してください。

ステップ 2 [Add] ダイアログボックスで、ドロップダウン リストから [Virtual KVM Policy] を選択して [Submit] をクリックします。

ステップ 3 [Policy Name] フィールドに名前を入力して、[Next] をクリックします。
また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[Server Details] ダイアログボックスが表示されます。このダイアログボックスでのタスクの実行については、既存の設定からのポリシーの作成, （27 ページ）を参照してください。

ステップ 4 [Enable vKVM] チェックボックスをオンにします。

ステップ 5 仮想サーバ プロパティを選択または入力するか、既存のプロパティを使用します。

ステップ 6 [Submit] をクリックします。

ステップ 7 [Submit Result] ダイアログボックスで、[OK] をクリックします。

VIC アダプタ ポリシー

さまざまなプロパティの設定の詳細については、『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』の「*Viewing VIC Adapter Properties*」の項を参照してください。

VIC アダプタ ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 [Hardware Policies] ページで、[Add] をクリックします。
このページに移動する方法の詳細については、ハードウェア ポリシーの作成, （3 ページ）を参照してください。

ステップ 2 [Add] ダイアログボックスで、ドロップダウン リストから [VIC Adapter Policy] を選択して [Submit] をクリックします。

ステップ 3 [Policy Name] フィールドに名前を入力して、[Next] をクリックします。
また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[Server Details] ダイアログボックスが表示されます。このダイアログボックスでのタスクの実行については、既存の設定からのポリシーの作成, （27 ページ）を参照してください。

ステップ 4 [Main] ダイアログボックスで [+] をクリックして、VIC アダプタ エントリをテーブルに追加します。

ステップ 5 [Add Entry to VIC Adapters] ダイアログボックスで、アダプタの詳細を入力または選択します。

- [vNIC]：デフォルト プロパティは eth0 および eth1 です。これらのプロパティは編集のみが可能であり、削除はできません。また、usNIC プロパティでもこれらのプロパティを使用できます。
- [vHBA]：デフォルト プロパティは fc0 および fc1 です。これらのプロパティは編集のみが可能であり、削除はできません。

ステップ 6 [Submit] をクリックします。

ステップ 7 [Submit Result] ダイアログボックスで、[OK] をクリックします。

ステップ 8 [Main] ダイアログボックスで [Submit] をクリックします。

ステップ 9 [Submit Result] ダイアログボックスで、[OK] をクリックします。

vMedia ポリシー

KVM コンソールおよび vMedia を使ってサーバに OS をインストールするために、Cisco IMC Supervisor を使用できます。1 つのサーバまたはサーバ セットのニーズに適合する、さまざまな OS イメージ用の vMedia マッピングを含む 1 つ以上の vMedia ポリシーを作成することができます。Cisco IMC Supervisor では、最大で 2 つの vMedia マッピングを設定できます。1 つは（CDD を介した）ISO ファイル用、もう 1 つは（HDD を介した）IMG ファイル用です。

さまざまな vMedia プロパティの設定の詳細については、『*Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide*』の「*Configuring Virtual Media*」の項を参照してください。

vMedia ポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 [Hardware Policies] ページで、[Add] をクリックします。
このページに移動する方法の詳細については、ハードウェア ポリシーの作成, （3 ページ）を参照してください。

ステップ 2 [Add] ダイアログボックスで、ドロップダウン リストから [vMedia Policy] を選択して [Submit] をクリックします。

ステップ 3 [Policy Name] フィールドに名前を入力して、[Next] をクリックします。
また、[Create policy from current configuration of the server] チェックボックスにマークを付けて [Next] をクリックすることもできます。これにより、[Server Details] ダイアログボックスが表示されます。このダイアログボックスでのタスクの実行については、既存の設定からのポリシーの作成, （27 ページ）を参照してください。

ステップ 4 [Main] ダイアログボックスで、[Enable vMedia] チェックボックスをオンにして vMedia を有効にし、[Enable Virtual Media Encryption] をオンにして vMedia 暗号化を有効にします。

ステップ 5 [Next] をクリックします。

ステップ 6 [Add CDD vMedia Mapping] チェックボックスをオンにして、CDD マッピングの詳細を入力します。

ステップ 7 [Next] をクリックします。

ステップ 8 [Add HDD vMedia Mapping] チェックボックスをオンにして、HDD マッピングの詳細を入力します。

ステップ 9 [Submit] をクリックします。

ステップ 10 [Submit Result] ダイアログボックスで、[OK] をクリックします。

（注）
- 現在、Cisco IMC Supervisor では [Low Power USB State] を設定できません。
- vMedia ポリシーを適用すると、ポリシーに vMedia マッピングが含まれない場合でも、それまでサーバに設定されていた既存の vMedia マッピングがすべて削除されます。

既存の設定からのポリシーの作成

すでに設定済みのサーバを使用してポリシーを作成することもできます。サーバ上の既存の設定を再使用すると、類似する設定を作成するのに必要な時間と労力を軽減できます。

（注） サーバの現在の設定からポリシーを作成するときには、サーバからパスワード フィールドが取得されません。

サーバの現在の設定からポリシーを作成するには、次の手順を実行します。

手順

ステップ 1 [Hardware Policies] ページで、[Add] をクリックします。
このページに移動する方法の詳細については、ハードウェア ポリシーの作成, （3 ページ）を参照してください。

ステップ 2 [Create policy from current configuration of the server] チェックボックスをオンにして、[Next] をクリックします。

ステップ 3 [Server Details] ダイアログボックスで、[Create policy from current configuration of the server] チェックボックスをオンにします。次の 2 つの方法でサーバの詳細を使用できます。

a) [Enter Server Details Manually] チェックボックスをオンにして、次のフィールドに入力します。

1 [Server IP] フィールドに IP アドレスを入力します。

2 既存のポリシーを選択するために [Use Credential Policy] チェックボックスをオンにして [Credential Policy] ドロップダウン リストからポリシーを選択するか、[Credential Policy] ドロップダウン リストの横にある [+] をクリックし、[Credential Policy Add Form] ダイアログボックスで詳細を入力して新規ポリシーを作成します。

3 [User Name] フィールドにサーバ ログイン名を入力します。

4 [Password] フィールドにサーバ ログイン パスワードを入力します。

5 [Protocol] ドロップダウン リストから http または https を選択します。

6 [Port] フィールドに、選択したプロトコルに関連付けられるポート番号を入力します。

b) [Select] をクリックして、設定の取得元となるサーバを選択します。

ステップ 4 [Next] をクリックします。
[Main] ダイアログボックスに進みます。ポリシーの作成を続けます。

ハードウェア ポリシーの適用

既存のポリシーをサーバに適用するには、次の手順を実行します。

手順

ステップ 1 メニュー バーで、[Policies] > [Manage Policies] を選択します。

ステップ 2 [Hardware Policies] タブを選択します。

ステップ 3 左側のペインから、適用するポリシーを選択します。

ステップ 4 上部にある利用可能なオプションから、[Apply] をクリックします。

ステップ 5 [Apply Policy] ダイアログボックスで、個別のサーバまたはラック サーバ グループ全体のどちらにポリシーを適用するかに応じて、ドロップダウン リストからサーバまたはサーバ グループを選択します。

ステップ 6 [Select] をクリックして、ポリシーの適用対象となるサーバ グループまたはサーバを選択します。

ステップ 7 ポリシー タスクの適用を後でスケジュールするには、[Schedule Later] チェックボックスをオンにします。

ステップ 8 [Schedule] ドロップダウン リストから既存のスケジュールを選択するか、[+] をクリックして新しいスケジュールを作成します。スケジュール作成の詳細については、スケジュールの作成 を参照してください。

（注） [Policies] > [Manage Schedules] の順に移動して、スケジュールを選択し、[View Scheduled Tasks] をクリックしてスケジュールされたタスクを表示するか、または [Remove Scheduled Tasks] をクリックしてスケジュールされたタスクを削除できます。

ステップ 9 [Submit] をクリックします。

ステップ 10 [Submit Result] ダイアログボックスで、[OK] をクリックします。

指定したサーバ セットにポリシーを適用するプロセスが開始します。ポリシーの種類、およびポリシーが適用されるサーバへのネットワーク接続に応じて、このプロセスに数分かかる場合があります。

ハードウェア ポリシーでの一般タスク

既存のポリシーのサーバ マッピング詳細を編集、削除、複製、または表示するには、次の手順を実行します。

手順

ステップ 1 メニュー バーで、[Policies] > [Manage Policies and Profiles] を選択します。

ステップ 2 [Hardware Policies] タブを選択します。

ステップ 3 [Hardware Policies] ページで、左側ペインのポリシーを展開して、ポリシーを選択します。オプションで次の手順を実行することができます。

a) （任意） ポリシーを削除するには、[Delete] をクリックします。[Delete Policy] ダイアログボックスで [Select] をクリックし、削除するポリシーを選択します。[Select] および [Submit] をクリックします。
ポリシーがサーバに関連付けられていても、選択した 1 つ以上のポリシーを削除できます。プロファイルに関連付けられたポリシーを削除しようとすると、エラーになります。

b) （任意） ポリシーを変更するには、[Properties] をクリックし、必要に応じてプロパティを変更します。
ポリシー名を変更するときには、すでに存在する名前を指定しないでください。

c) （任意） ポリシーを複製するには、[Clone] をクリックして、選択したポリシーの詳細を新しいポリシーにコピーします。

d) （任意） [View Details] をクリックすると、すでに適用したポリシーのステータス、およびポリシーが適用されたサーバ IP アドレスが表示されます。ポリシーが正常に適用されない場合、[Status Message] 列にエラー メッセージが表示されます。

ステップ 4 サーバまたはサーバ グループにポリシーを適用するには、[Apply] をクリックします。プロファイルを適用する方法の詳細については、ハードウェア ポリシーの適用, （28 ページ）を参照してください。

ステップ 5 状況に応じて [Submit] または [Close] をクリックします。

ハードウェア プロファイル

複数のポリシーを組み合わせて、ハードウェア プロファイルが形成されます。たとえば、1 つのラック ハードウェア プロファイル設定の詳細情報を複数のラックマウント サーバに適用することができます。いくつかの特定のラックマウントサーバにこのハードウェアプロファイルを関連付けることができます。これにより、複数のサーバにわたって設定の一貫性と反復可能性が確保されます。プロファイルを定義して使用すると、類似する設定が多数のサーバに適用されるため、一貫性、制御、予測可能性、自動化が促進されます。

次のワークフローは、Cisco IMC Supervisor でハードウェア プロファイルを使用する方法を示しています。

1. ハードウェア プロファイルを作成します。次のいずれかの方法でプロファイルを作成できます。
   a. 新しいプロファイルを作成します。新しいプロファイルの作成方法の詳細については、ハードウェア プロファイルの作成, （30 ページ）を参照してください。
   b. サーバ上の既存の設定からプロファイルを作成します。サーバ上の既存の設定からプロファイルを作成する方法の詳細については、既存の設定からのプロファイルの作成, （31 ページ）を参照してください。
2. サーバでプロファイルを適用します。プロファイルを適用する方法の詳細については、ハードウェア プロファイルの適用, （33 ページ）を参照してください。
3. プロファイルで、必要に応じて次のオプション作業を実行します。
   a. Edit
   b. Delete
   c. Clone

   また、特定のプロファイルにマップされるサーバのリストを表示して、このプロファイルに関連付けられているポリシーの詳細を表示することもできます。これらのタスクの実行方法の詳細については、ハードウェア プロファイルでの一般タスク, （33 ページ）を参照してください。

ハードウェア プロファイルの作成

ハードウェア プロファイルを作成するには、次の手順を実行します。

手順

ステップ 1 メニュー バーで、[Policies] > [Manage Policies and Profiles] を選択します。

ステップ 2 [Hardware Profiles] タブを選択します。

ステップ 3 [Add] をクリックします。

ステップ 4 [Hardware Profile] ダイアログボックスの [Profile Name] フィールドで、作成するプロファイルの名前を入力します。

ステップ 5 [Next] をクリックするか、[Create profile from current configuration of the server] チェックボックスをオンにして [Next] をクリックします。
[Server Details] ウィンドウでタスクを実行するには、既存の設定からのプロファイルの作成を参照してください。

ステップ 6 [Profile Entities] ダイアログボックスで [+] をクリックして、プロファイル エントリを追加します。また、編集アイコンや削除アイコンをクリックして、既存のエントリを編集および削除することもできます。

ステップ 7 [Add Entry to Profile Name] ダイアログボックスで、[Policy Type] を選択します。

ステップ 8 既に作成済みのポリシーの名前をリストする [Policy Name] ドロップダウン リストから、ポリシー名を選択します。
[Policy Name] の横にある [+] をクリックすると、既に選択したポリシー タイプに基づく新しいポリシーを作成できます。ポリシーの作成の詳細については、以下を参照してください。 ハードウェア ポリシーの作成, （3 ページ）

ステップ 9 [Submit] をクリックします。

ステップ 10 [Submit Result] 確認ダイアログボックスで、[OK] をクリックします。

ステップ 11 [Profile Entities] ダイアログボックスで [Submit] をクリックします。

ステップ 12 [Submit Result] 確認ダイアログボックスで、[OK] をクリックします。

次の作業

また、プロファイルを編集、削除、複製したり、選択されたプロファイルにマップされるサーバを表示したりすることもできます。これらのタスクの実行については、以下を参照してください。
ハードウェア プロファイルでの一般タスク, （33 ページ）

既存の設定からのプロファイルの作成

すでに設定済みのサーバを使用してプロファイルを作成することもできます。サーバ上の既存の設定を再使用すると、類似する設定を作成するのに必要な時間と労力を軽減できます。

（注） サーバの現在の設定からプロファイルを作成するときには、サーバからパスワード フィールドが取得されません。

サーバの現在の設定からプロファイルを作成するには、次の手順を実行します。

手順

ステップ 1 メニュー バーで、[Policies] > [Manage Policies and Profiles] を選択します。

ステップ 2 [Hardware Profiles] タブを選択します。

ステップ 3 [Add] をクリックします。

ステップ 4 プロファイルの名前を [Name] フィールドに入力します。

ステップ 5 [Create profile from current configuration of the server] チェックボックスをオンにします。次の方法でサーバの詳細を使用できます。

a) [Enter Server Details Manually] チェックボックスをオンにして、次のフィールドに入力します。

1. [Server IP] フィールドに IP アドレスを入力します。
2. 既存のポリシーを選択するために [Use Credential Policy] チェックボックスをオンにして [Credential Policy] ドロップダウン リストからポリシーを選択するか、[Credential Policy] ドロップダウン リストの横にある [+] をクリックし、[Credential Policy Add Form] ダイアログボックスで詳細を入力して新規ポリシーを作成します。
3. [User Name] フィールドにサーバ ログイン名を入力します。
4. [Password] フィールドにサーバ ログイン パスワードを入力します。
5. [Protocol] ドロップダウン リストから http または https を選択します。
6. [Port] フィールドに、選択したプロトコルに関連付けられるポート番号を入力します。
7. [Select] をクリックし、ポリシーを選択して [Select] をクリックします。

b) [Select] をクリックして、設定の取得元となるサーバを選択します。

c) [Select] をクリックし、ポリシーを選択して、[Select] をクリックします。

ステップ 6 [Next] をクリックします。

ステップ 7 [Profile Entities] ダイアログボックスで [+] をクリックして、プロファイル名にエントリを追加します。
[Profile Name] テーブルから既存のエントリを削除するには、[x] をクリックします。

ステップ 8 [Submit] をクリックします。

ステップ 9 [Submit Result] ダイアログボックスで、[OK] をクリックします。

ハードウェア プロファイルの適用

ハードウェア プロファイルをラック サーバに適用するには、次の手順を実行します。

手順

ステップ 1 メニュー バーで、[Policies] > [Manage Policies and Profiles] を選択します。

ステップ 2 [Hardware Profiles] タブを選択します。

ステップ 3 既存のハードウェア プロファイルを選択し、[Apply] をクリックします。

ステップ 4 [Apply Profile] ダイアログボックスで、個別のサーバまたはラック サーバ グループ全体のどちらにプロファイルを適用するかに応じて、ドロップダウン リストからサーバまたはサーバ グループを選択します。

ステップ 5 [Select] をクリックして、プロファイルの適用対象となるサーバ グループまたはサーバを選択します。

ステップ 6 プロファイル タスクの適用を後でスケジュールするには、[Schedule Later] チェックボックスをオンにします。

ステップ 7 [Schedule] ドロップダウン リストから既存のスケジュールを選択するか、または [+] をクリックして新しいスケジュールを作成します。スケジュール作成の詳細については、スケジュールの作成を参照してください。

（注） [Policies] > [Manage Schedules] の順に移動して、スケジュールを選択し、[View Scheduled Tasks] をクリックしてスケジュールされたタスクを表示するか、または [Remove Scheduled Tasks] をクリックしてスケジュールされたタスクを削除できます。

ステップ 8 [Submit] をクリックします。

ステップ 9 [Submit Result] 確認ダイアログボックスで、[OK] をクリックします。
指定したサーバ セットにプロファイルを適用するプロセスが開始します。プロファイルの種類、およびプロファイルが適用されるサーバへのネットワーク接続に応じて、このプロセスに数分かかる場合があります。

ハードウェア プロファイルでの一般タスク

既存のプロファイルのサーバ マッピング詳細を編集、削除、複製、または表示するには、次の手順を実行します。

手順

ステップ 1 メニュー バーで、[Policies] > [Manage Policies and Profiles] > [Hardware Profiles] を選択します。

ステップ 2 左側ペインの [Hardware Profile] を展開して、[Hardware Profiles] ページで、プロファイルを選択します。オプションで次の作業を行うことができます。

a) （任意） プロファイルを削除するには、[Delete] をクリックします。[Delete Profile] ダイアログボックスの [Select] をクリックし、1 つ以上のプロファイルを選択して、[Select] をクリックします。[Submit] をクリックするとプロファイルが削除されます。
サーバに関連付けられていてもプロファイルを削除できます。

b) （任意） プロファイルを変更するには、プロファイルを選択し、[Edit] をクリックして、必要に応じてプロパティを変更します。
プロファイル名を変更するときには、すでに存在する名前を指定しないでください。

c) （任意） 既存のプロファイルの詳細を新しいプロファイルにコピーするには、[Clone] をクリックします。

d) （任意） サーバまたはサーバ グループにプロファイルを適用するには、[Apply] をクリックします。プロファイルを適用する方法の詳細については、ハードウェア プロファイルの適用，（33 ページ）を参照してください。

e) （任意） [View Details] をクリックすると、すでに適用したプロファイルのステータス、およびプロファイルが適用されたサーバ IP アドレスが表示されます。プロファイルが正常に適用されない場合、[Status Message] 列にエラー メッセージが表示されます。

ステップ 3 状況に応じて [Submit] または [Close] をクリックします。

タグ ライブラリ

オブジェクトにラベルを割り当てる場合にタグ付けを行います。管理者は、Cisco IMC Supervisor のリソース グループやユーザ グループなどのオブジェクトにタグを付けることを決定できます。ラック アカウントなどのカテゴリにタグを割り当てることができます。また、選択したカテゴリの特定のタイプのアカウントにタグを適用することもできます。

[Tag Library] の唯一のタブには、次の詳細が表示されます。

フィールド	説明
Name	タグ ライブラリのユーザ定義名。
Description	タグ ライブラリのユーザ定義の簡単な説明。
Type	文字列または整数。
Possible Tag Values	ユーザ定義のタグ値。
Applies To	ラックマウント サーバまたはユーザ。

タグ ライブラリの作成

タグ ライブラリを作成する場合は、次の手順を実行します。

手順

ステップ 1 メニュー バーで、[Policies] > [Tag Library] を選択します。

ステップ 2 [Create] をクリックします。

ステップ 3 [Create Tag] ダイアログボックスで、[Tag Details] の次のフィールドに入力します。

フィールド	説明
[Name] フィールド	タグの記述名。
[Description] フィールド	（オプション）タグの説明。
[Type] ドロップダウン リスト	文字列または整数を選択します。
[Possible Tag Values] フィールド	タグに使用できる値。

ステップ 4 [Next] をクリックします。

ステップ 5 [Applicability Rules] ペインで、次の手順を実行します。

名前	説明
[Taggable Entities] フィールド	タグを適用する必要があるエンティティを選択します。 エンティティを追加するには、以下を実行します。 **1** [+] アイコンをクリックします。 **2** [Category] ドロップダウン リストから、カテゴリを選択します。次のいずれかを指定できます。 • Physical_Compute • Administration **3** テーブルからタグ付け可能なエンティティを選択します。 **4** [Submit] をクリックします。 （注） タグは、タグ付け可能なエンティティの設定に応じてそれぞれのカテゴリの下に表示されます。

ステップ 6 確認ダイアログボックスで、[OK] をクリックします。

ステップ 7 [Create Tag] ダイアログボックスで、[Submit] をクリックします。

ステップ 8 [OK] をクリックします。

（注） 使用可能なオプションをクリックすることで、タグおよびタグの関連付けの詳細を複製、編集、削除、表示するといった、さまざまなタスクを実行できます。