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 **[Policies]** > **[Manage Policies and Profiles]** を選択します。

ステップ 2 [Manage Policies and Profiles] ページで、[Credential Policies] をクリックします。

ステップ 3 [Add] をクリックします。

ステップ 4 **[Add Credential Policy (クレデンシャル ポリシーの追加)]** 画面で、次のフィールドに入力します。

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 5 [送信（Submit）] をクリックします。

（注） 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

ポリシーとは、Cisco IMCでのさまざまな属性の設定を定義するメカニズムです。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で説明します。

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。
    1. 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。
    2. 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 （38 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 （40 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。
    1. Edit
    2. 削除
    3. Clone
    4. 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 （41 ページ）を参照してください。
    5. 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 （45 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 **[Policies]** > **[Manage Policies and Profiles]** を選択します。

ステップ 2 [Manage Policies and Profiles] ページで、[Hardware Policies] をクリックします。

ステップ 3 [Add] をクリックします。

ステップ 4 [Add] 画面で、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、次の表でポリシー タイプを選択してください。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。

（注） ポリシー作成用の Cisco UCS S3260 プラットフォームを選択するためのチェックボックスが導入されています。このオプションは、デフォルトで無効です。Cisco UCS S3260 のポリシーを作成する必要がある場合、このチェックボックスをオンにして、同様に有効にする必要があります。

Policy Type	『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 （12 ページ）	*IPMI* の設定
LDAP ポリシー （14 ページ）	*LDAP* サーバの設定
レガシー ブート順序ポリシー （15 ページ）	サーバのブート順
ネットワーク構成ポリシー （16 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 （20 ページ）	ネットワーク セキュリティの設定
NTP ポリシー （21 ページ）	ネットワーク タイム プロトコル設定の設定
パスワードの有効期限ポリシー （22 ページ）	パスワードの有効期限切れ
高精度のブート順序ポリシー （23 ページ）	高精度ブート順の設定
電力復元ポリシー （24 ページ）	電力復元ポリシーの設定
RAID ポリシー （25 ページ）	ストレージ アダプタの管理
Serial over LAN ポリシー （28 ページ）	*Serial over LAN* の設定
SNMP ポリシー （29 ページ）	*SNMP* の設定
SSH ポリシー （30 ページ）	*SSH* の設定

Policy Type	『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』内のセクション
ユーザ ポリシー （31 ページ）	ローカル ユーザの設定
VIC アダプタ ポリシー （34 ページ）	*VIC* アダプタのプロパティの表示
仮想 KVM ポリシー （33 ページ）	仮想 *KVM* の設定
vMedia ポリシー （36 ページ）	仮想メディアの設定
ゾーン分割ポリシー （37 ページ）	『*Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide for S3260 Storage Servers*』の「*Dynamic Storage*」。

次のタスク

サーバにポリシーを適用します。「ハードウェア ポリシーの適用 （40 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 ポリシーを作成できます。サーバの BIOS ポリシーを指定しない場合、BIOS 設定はデフォルト値のセット (新品のベア メタル サーバの場合)、あるいは以前に Cisco IMC を使用して設定した値のセットになります。BIOS ポリシーを指定した場合、ポリシーの値がサーバに設定されている値に置き換わります。

BIOS のプロパティの設定に関する詳細は、『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』の「*Configuring BIOS Settings*」を参照してください。

手順

ステップ 1 [Hardware Policies] を選択したら、[Add] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [Add] 画面で、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] 画面が表示されます。既存の設定からのポリシーの作成 （38 ページ）を参照してください。

ステップ 4 Cisco UCS S3260 サーバ用のポリシーの場合は、[Cisco UCS S3260] 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 5 [Main] 画面で、主要な BIOS プロパティ（[Boot Option Retry]、[Post Error Pause]、および [TPM Support] ドロップダウンリストのエントリなど）の値を選択します。[Power ON Password Support] ドロップダウン リストでは電源オン時のパスワード サポートを有効または無効にすることができます。デフォルトのプラットフォーム設定を選択することもできます。これを有効にすると、設定の変更や BIOS セットアップへのアクセスなど、サーバに変更を加えることができません。

（注） CIMC UI を使用し、[BIOS Configuration] 画面で BIOS パスワードが設定されていることを確認します。

ステップ 6 [Advanced] 画面で、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 7 [Server Management] 画面で、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。

（注） BIOS ポリシーには、すべての使用可能なプラットフォームのためのトークンが表示されます。

- 属性が特定のサーバプラットフォームに対して有効でない場合、トークンは無視されます。たとえば、Power On Password Support BIOS トークンは、3.x ファームウェアを実行しているサーバにのみ適用されます。このトークンは、3.x より前のファームウェアを実行しているサーバに適用されると、無視されます。
- 属性がターゲットプラットフォームに存在しており、その値が該当しない場合、エラーが発生します。たとえば、Extended APIC BIOS トークンには Enabled および Disabled という値がありますが、これは、プラットフォーム A に基づくサーバ モデルにのみ該当します。ただし、このトークンが プラットフォーム B のサーバ モデルに適用されると、xml 解析エラーが表示されます。

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 （25 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] を選択したら、[Add] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [Add] 画面で、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] 画面で、[RAID Level] ドロップダウン リストから RAID レベルを選択し、[Next] をクリックします。

ステップ 5 [Local Disk Configuration] 画面で、[+] 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。

（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 ポリシーは、Cisco UCS S3260 ラック サーバでは使用できません。

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] を選択したら、[Add] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [Add] 画面で、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] 画面が表示されます。既存の設定からのポリシーの作成 （38 ページ）を参照してください。

ステップ 4 [Configure Cards] ページで、次のフィールドに入力します。

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。
[Mirror] オプション ボタン	[Enable Virtual Drive] チェックボックスをオンにして [Hypervisor] 仮想ドライブを有効にするか、または [Erase Virtual Drive] チェックボックスをオンにして仮想ドライブを削除します。

フィールド	説明
[Util] オプション ボタン	[Enable Virtual Drive] チェックボックスをオンにして仮想ドライブ（[SCU]、[Hypervisor]、[Drivers]、[HUU]、および [User Partition]）を有効にするか、または [Erase Virtual Drive] チェックボックスをオンにして仮想ドライブを削除します。 （注） 複数の仮想ドライブを選択できます。
[Not Applicable] ラジオ ボタン	[Enable Virtual Drive] チェックボックスをオンにして仮想ドライブ（[SCU]、[HV]、[Drivers]、および [HUU]）を有効にします。 （注） • 複数の仮想ドライブを選択できます。 • [Erase Virtual Drive] チェックボックスは使用できません。
[Partition Name] フィールド（[Mirror] および [Util] モードでのみ使用可能）	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。

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. 新しいポリシーの設定が適用されます。このステップで何らかの障害が発生した場合、既存の設定はポリシーに適用される前に失われます。

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] を選択したら、[Add] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [Add] 画面で、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] 画面が表示されます。既存の設定からのポリシーの作成 （38 ページ）を参照してください。

ステップ 4 ラックマウント サーバ用にこのポリシーを作成している場合は、次の手順を実行します。

a) [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。

b) [Next] をクリックします。

c) [Confirm] 画面で、[Submit] をクリックします。
[Hardware Policies] ページの [Server Platform] カラムにラックマウント サーバが一覧表示されます。

ステップ 5 Cisco UCS S3260 サーバ用のポリシーの場合は、[Cisco UCS S3260] 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 6 [CMC Settings] 画面で、必要に応じて、CMC 1 と CMC 2 の両方の [Enable IPMI Over LAN] チェックボックスをオンにします。

ステップ 7 [Next] をクリックします。

ステップ 8 [BMC Settings] 画面で、必要に応じて、BMC 1 と BMC 2 の両方の [Enable IPMI Over LAN] チェックボックスをオンにします。

ステップ 9 [Confirm] 画面で、[Submit] をクリックします。

You can see the Cisco UCS S3260 Dense Storage Rack Server listed in the Server Platform column in the **[Hardware Policies (ハードウェア ポリシー)]** ページの [Server Platform (サーバ プラットフォーム)] カラムにCisco UCS S3260 高密度ストレージ ラック サーバが一覧表示されます。

LDAP ポリシー

Cisco C シリーズ サーバと E シリーズ サーバは LDAP をサポートしています。Cisco IMC Supervisor は LDAP ポリシーを使用したサーバでの LDAP 設定をサポートしています。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* シリーズ サーバの統合管理コントローラ *GUI* の構成ガイド（*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。

手順

ステップ 1 [Hardware Policies] を選択したら、[Add] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [Add] 画面で、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] 画面が表示されます。既存の設定からのポリシーの作成 （38 ページ）を参照してください。

ステップ 4 Cisco UCS S3260 サーバ用のポリシーの場合は、[Cisco UCS S3260] 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 5 [Main] 画面で、LDAP のプロパティを入力し、[Next] をクリックします。

ステップ 6 [Configure LDAP Servers] 画面で、LDAP サーバの詳細を入力し、[Next] をクリックします。

ステップ 7 [Group Authorization] 画面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 8 [Add Entry to LDAP Groups] 画面で、グループの詳細を入力し、[Submit] をクリックします。

（注）
- サーバに設定されている既存の LDAP ロール グループはすべて削除され、ポリシーで設定したロール グループに置き換えられます。ポリシーにロール グループを追加していない場合、サーバ上の既存のロール グループは単純に削除されます。
- **[Nested Group Search Depth (検索するグループのネスト レベル)]** は、Cisco IMC バージョン 2.0(4c) 以降のみに適用されます。バージョン 2.0(4c) より古い Cisco IMC が稼働しているサーバでポリシーを使用し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。「高精度のブート順序ポリシー （23 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。

（注） レガシー ブート順序ポリシーは、Cisco UCS S3260 ラック サーバでは使用できません。

手順

ステップ 1 [Hardware Policies] を選択したら、[Add] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [Add] 画面で、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] 画面が表示されます。既存の設定からのポリシーの作成 （38 ページ）を参照してください。

ステップ 4 [Main] 画面で [+] 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] 画面で [Submit] をクリックします。

（注） このポリシーは 2.0 より前の Cisco IMC バージョンにのみ適用されます。より高い Cisco IMC バージョンを実行しているサーバに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、サーバの以下のネットワーク設定を指定できるネットワーク構成ポリシーを作成できます。

- DNS ドメイン
- IPv4 および IPv6 用の DNS サーバ
- VLAN コンフィギュレーション

各種のネットワーク設定プロパティに関する詳細は、『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。

手順

ステップ 1 [Hardware Policies] を選択したら、[Add] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 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] ウィンドウが表示されます。「既存の設定からのポリシーの作成 （38 ページ）」を参照してください

ステップ 4 ラックマウント サーバ用にこのポリシーを作成している場合は、次の手順を実行します。

a) [Main] 画面で、次のフィールドに入力します。

フィールド	説明
[Common Properties]	
[Use Dynamic DNS] チェックボックス	ダイナミック DNS は、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。 Cisco IMC Supervisor
[Use Dynamic DNS] チェックボックスをオンにした場合	
[**Dynamic DNS Update Domain**] フィールド	ドメインを指定できます。ドメインは、メイン ドメインまたはサブ ドメインのどちらでも可です。このドメイン名は、DDNS 更新のため Cisco IMC Supervisor のホスト名に付加されます。
IPv4 のプロパティ	
[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。
[Obtain DNS Server Addresses from DHCP] チェックボックスをオフにした場合	
[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 のプロパティ	
[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。
[Obtain DNS Server Addresses from DHCP] チェックボックスをオフにした場合	
[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。
[VLAN Properties]	
[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。
[Enable VLAN] チェックボックスをオンにした場合	
[VLAN ID] フィールド	VLAN ID。
[Priority] フィールド	VLAN でのこのシステムのプライオリティ。

b) [Next] をクリックします。
c) [Confirm] 画面で、[Submit] をクリックします。

[Hardware Policies] ページの [Server Platform] カラムにラックマウント サーバが一覧表示されます。

ステップ 5 Cisco UCS S3260 サーバ用のポリシーの場合は、[Cisco UCS S3260] 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 6 [Main] 画面で、次のフィールドに入力します。

フィールド	説明
[Common Properties]	
[Use Dynamic DNS] チェックボックス	ダイナミック DNS は、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。 Cisco IMC Supervisor
[Use Dynamic DNS] チェックボックスをオンにした場合	
[**Dynamic DNS Update Domain**] フィールド	ドメインを指定できます。ドメインは、メイン ドメインまたはサブ ドメインのどちらでも可です。このドメイン名は、DDNS 更新のため Cisco IMC Supervisor のホスト名に付加されます。
IPv4 のプロパティ	
[Use DHCP] チェックボックス	オンにすると、[Obtain DNS Server Addresses from DHCP] チェックボックスが表示されます。
[Obtain DNS Server Addresses from DHCP] チェックボックス	オンにすると、DNS の DHCP が有効になります。
[Obtain DNS Server Addresses from DHCP] チェックボックスをオフにした場合	
[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 のプロパティ	
[Enable IPv6] チェックボックス	オンにすると、[Use DHCP] チェックボックスが表示されます。
[Use DHCP] チェックボックス	オンにすると、[Obtain DNS Server Addresses from DHCP] チェックボックスが表示されます。
[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。
[Use DHCP] チェックボックスをオフにした場合	

フィールド	説明
[Management IP Address] フィールド	管理 IP アドレスを入力します。
[**Prefix Length**] フィールド	プレフィックス長の文字数を入力します。
[Gateway] フィールド	ゲートウェイの IP アドレスを入力します。
[Obtain DNS Server Addresses from DHCP] チェックボックスをオフにした場合	
[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。
[VLAN Properties]	
[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。
[Enable VLAN] チェックボックスをオンにした場合	
[VLAN ID] フィールド	VLAN ID。
[Priority] フィールド	VLAN でのこのシステムのプライオリティ。

ステップ 7 [Next] をクリックします。

ステップ 8 [CMC Settings] 画面で、必要に応じて、CMC 1 と CMC 2 の両方の以下のフィールドに入力します。

フィールド	説明
[Hostname] フィールド	サーバのホスト名。
[IPv4 Address] フィールド	IPv4 の IP アドレス。
[IPv6 Address] フィールド	IPv6 の IP アドレス。

ステップ 9 [Next] をクリックします。

ステップ 10 [BMC Settings] 画面で、必要に応じて BMC 1 と BMC 2 の両方の以下のフィールドに入力します。

フィールド	説明
[Hostname] フィールド	サーバのホスト名。
[IPv4 Address] フィールド	IPv4 の IP アドレス。
[IPv6 Address] フィールド	IPv6 の IP アドレス。

ステップ 11 [Next] をクリックします。

ステップ 12 [Confirm] 画面で、[Submit] をクリックします。

注意 Cisco IMC Supervisor とラック サーバの間のネットワークの DHCP 設定に依存する通信が遮断されないようにするため、次の設定を使用するときには注意してください

DNS IP アドレスを取得するために DHCP を使用している場合、サーバの管理 IP アドレスに DHCP を使用するために（このポリシーが適用される）ラック サーバも設定されます。

ネットワーク セキュリティ ポリシー

Cisco IMC Supervisor IP ブロッキングをネットワーク セキュリティとして使用します。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。

ネットワーク セキュリティ ポリシーを作成するときに 4 つの IP フィルタリング プロパティを設定できます。IP フィルタリングでは、選択した一連の IP がサーバにアクセスできます。4 つのフィルタ フィールドのいずれも、単一の IP アドレスまたはハイフンで区切った IP アドレス範囲を入力できます。IP アドレスは、IPv4 または IPv6 アドレスを使用できます。

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] を選択したら、[Add] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [Add] 画面で、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] ウィンドウが表示されます。既存の設定からのポリシーの作成 （38 ページ）を参照してください。

ステップ 4 Cisco UCS S3260 サーバ用のポリシーの場合は、[Cisco UCS S3260] 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 5 [IP Blocking] ウィンドウで、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 6 [Next] をクリックします。

ステップ 7 [IP Filtering] 画面で、[Enable IP Filtering] チェックボックスをオンにして IP を有効にし、IP アドレスを 1 つまたは範囲で入力します。

（注） [Filter 1] は、デフォルトで Cisco IMC Supervisor の IP アドレスを表示します。

ステップ 8 [送信（Submit）] をクリックします。

NTP ポリシー

NTP サービスにより、Cisco IMC Supervisor が管理するサーバが NTP サーバと時刻を同期するように設定できます。デフォルトでは NTP サーバは Cisco IMC Supervisor で動作しません。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 は設定された NTP サーバと管理されているサーバ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] を選択したら、[Add] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [Add] 画面で、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] 画面が表示されます。既存の設定からのポリシーの作成 （38 ページ）を参照してください。

ステップ 4 Cisco UCS S3260 サーバ用のポリシーの場合は、[Cisco UCS S3260] 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 5 [Main] 画面で、[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 6 [Submit] 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。

パスワードの有効期限ポリシー

パスワードの有効期限を設定することができ、その期限を過ぎるとパスワードは期限切れになります。管理者として、この時間を日数で設定できます。この設定は、すべてのユーザに共通です。ユーザは、ユーザポリシーの一部として構成を設定して派生させ、パスワード有効期限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 Password Expiry for Users*」の項を参照してください。

パスワード有効期限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] を選択したら、[Add] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [Add] 画面で、ドロップダウン リストから [Password Expiration 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ます。

ステップ 4 [Main] 画面で、次のフィールドに入力します。

フィールド	説明
[Enable Password Expiry] チェックボックス	指定したパスワードの有効期限を有効にするには、このチェックボックスをオンにして、次の項目を入力します。 [Password Expiry Duration]：パスワードが期限切れになる日数を設定します。
[Password History] フィールド	パスワード履歴を表示するときに表示される発生数を設定します。
[Notification Period] フィールド	パスワードの有効期限について通知されるまでの日数を設定します。
[Grace Period] フィールド	パスワードの期限が切れるまでの猶予期間を設定します。

ステップ 5 [Submit] をクリックします。

（注）
- 既存のポリシーを選択し、[Properties] または [Delete] をクリックして、[More Actions] ドロップダウンリストからポリシーを編集または削除することもできます。
- このポリシーは、ユーザ ポリシーとともに適用する必要があります。パスワード有効期限ポリシーを個別に適用することはできません。
- E シリーズ サーバは、パスワード有効期限ポリシーをサポートしていません。

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、ブート順およびブート モードの変更、各デバイス タイプ下への複数のデバイスの追加、ブート順の並び替え、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に対して作成できます。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] を選択したら、[Add] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [Add] ウィンドウで、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] ウィンドウが表示されます。既存の設定からのポリシーの作成 （38 ページ）を参照してください。

ステップ 4 Cisco UCS S3260 サーバ用のポリシーの場合は、[Cisco UCS S3260] 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 5 [Main] ウィンドウで、[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 6 [+] 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。

（注） **HTTP ブート**は、CIMC バージョン4.1（3b）からサポートされます。

ステップ 7 [Add Entry to Select Devices] ページで、[Submit] をクリックします。

ステップ 8 サーバが一回起動する必要があるデバイスを設定するには、[Configure One Time Boot Device] チェックボックスをオンにします。

ステップ 9 [One Time Boot Device] ドロップダウン リストからデバイスを選択します。

（注） [Configure One Time Boot Device] は、3.0(1c) より古いバージョンの CIMC には適用されません

ステップ 10 選択したサーバでワンタイムブートデバイスが更新された後でサーバをリブートするときは、[Reboot On Update] チェックボックスをオンにします。

ステップ 11 [送信（Submit）] をクリックします。

電力復元ポリシー

C シリーズまたは E シリーズ サーバに設定されている電力復元ポリシーの値を変更し、この際にサーバの Cisco IMC にログインする必要がないようにする場合に、このポリシーを作成します。

（注） ENCS サーバでこのポリシーを作成することはできません。

手順

ステップ 1 [Hardware Policies] を選択したら、[Add] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 **[Add (追加)]** 画面で、ドロップダウンリストから **[Power Restore Policy (電力復元ポリシー)]** を選択して **[Submit (送信)]** 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] 画面が表示されます。既存の設定からのポリシーの作成 （38 ページ）を参照してください。

ステップ 4 Cisco UCS S3260 サーバ用のポリシーの場合は、[Cisco UCS S3260] 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 5 **[Power Restore Policy (電力復元ポリシー)]** から設定を選択します。

次のいずれかのオプションを使用できます。

- **Power Off**
- **電源オン**

  このオプションを選択すると、**[Power Delay Type (電源遅延タイプ)]** フィールドが表示されます。このオプションを使用できるのは Cisco UCS C シリーズ サーバだけです。

- **最後の状態の復元**

ステップ 6 **[Power Delay Type (電源遅延タイプ)]** ドロップダウン リストから値を選択します。

次のいずれかのオプションを使用できます。

- **固定**: このオプションを選択すると、**[Power Delay Value (電源遅延値)]** フィールドが表示されます。
- **ランダム**: このオプションを選択した場合、**[Power Delay Value (電力遅延値)]** フィールドは表示されません。

ステップ 7 **[Power Delay value (電力遅延値)]** フィールドに 0 ~ 240 秒の値を指定します。

ステップ 8 [送信（Submit）] をクリックします。

次のタスク

このポリシーを適用する必要があります。詳細については、ハードウェア ポリシーの適用 （40 ページ）を参照してください。

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) 以降。

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] を選択したら、[Add] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [Add] ウィンドウで、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] ウィンドウが表示されます。既存の設定からのポリシーの作成 （38 ページ）を参照してください。

ステップ 4 Cisco UCS S3260 サーバ用のポリシーの場合は、[Cisco UCS S3260] 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 5 [Drive Security] ウィンドウで、[Configure Drive Security] チェックボックスをオンにしてドライブのセキュリティを設定します。

重要 **[サーバの現在の設定からポリシーを作成する (Create policy from current configuration of the server)]** チェック ボックスをオンにして、セキュリティ キー ID などのセキュリティ プロパティがサーバに関連付けられているすべてのコントローラ スロットに共通している場合にのみ、ポリシーのドライブ セキュリティ プロパティが取得されます。セキュリティ キー ID がサーバ内のすべてのコントローラで共通でない場合は、ドライブセキュリティ設定の取得に失敗し、その後RAIDポリシーは作成されません。

ステップ 6 [Enable Drive Security] または [Disable Drive Security] ラジオ ボタンを選択して、ドライブのセキュリティを有効または無効にします。

（注） ドライブのセキュリティを有効にすると、セキュリティ キーの詳細を入力できるようになります。

ステップ 7 [Enable Drive Security] を選択し、次のフィールドに入力します。

フィールド	説明
[Local Key Management] チェックボックス	このチェックボックスは、デフォルトでオンになっています。
[Security Key] フィールド	セキュリティ キーを入力します。
[Security Key Identifier] フィールド	セキュリティ キー識別子を入力します。
[Confirm Security Key] フィールド	先ほど入力したセキュリティ キーを確認します。
[Current Security Key] フィールド	セキュリティ キーを変更する場合のみ、キーを入力します。

（注） Cisco IMC Supervisor が RAID ポリシーとセキュリティ キーをエクスポートすると、Cisco IMC Supervisor によるセキュリティ キーの露出を防ぐため、セキュリティ キー パラメータは空のままになります。このため、値は手動で入力する必要があります。

ステップ 8 [Virtual Drive Configuration] ダイアログボックスで [+] をクリックして、サーバ上に設定する仮想ドライブを追加します。

サーバ上のすべてのコントローラ スロットの仮想ドライブと、それらの仮想ドライブ上の対応するディスク グループ ポリシーが取得され、ユーザー インターフェイスに表示されます。

ステップ 9 [+] をクリックして、仮想ドライブ テーブルにエントリを追加します。[Add Entry to Virtual Drives] ページで、次のように入力します。

フィールド	説明
[Virtual Drive Name] フィールド	指定したパスワードの有効期限を有効にするには、このチェックボックスをオンにして、次の項目を入力します。 [Password Expiry Duration]：パスワードが期限切れになる日数を設定します。
仮想ドライブ サイズ	各ストライプのサイズ（KB 単位）。 M2 RAID コントローラは 32K と 64K のみをサポートします。他の RAID コントローラは、64k、128k、256k、612k、および 1024k をサポートします。
[Disk Group Policy] ドロップダウン リスト	[Disk Group Policy] ドロップダウンリストから既存のディスク グループ ポリシーを選択するか、または [+] をクリックし、新しいディスク グループ ポリシーを追加してローカル ディスクを指定します。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。
[Access Policy] ドロップダウン リスト	表示されるオプションから選択します。
[Read Policy] ドロップダウン リスト	表示されるオプションから選択します。
[Write Policy] ドロップダウン リスト	表示されるオプションから選択します。
[IO Policy] ドロップダウン リスト	表示されるオプションから選択します。

フィールド	説明
[Drive Cache] ドロップダウン リスト	表示されるオプションから選択します。
[Expand to available] チェックボックス	ディスクで使用可能な最大容量を使用するために、仮想ドライブサイズを拡張します。
[Boot Drive] チェックボックス	ブート ドライブとして作成する仮想ドライブを設定します。 （注） 複数のブート ドライブを設定することはできません。
[Set disks in JBOD state to Unconfigured Good] チェックボックス	JBOD状態であるディスクを、仮想ドライブの作成に使用される前に未設定の良好状態に設定します。
[Enable Full Disk Encryption] チェックボックス	未使用の物理ドライブから仮想ドライブを作成します。

ステップ 10 [Submit] をクリックします。
作成した仮想ドライブは [Virtual Drives] テーブルで確認できます。

ステップ 11 [Delete existing Virtual Drives] チェックボックスをオンにして、サーバ上の既存のすべての仮想ドライブを削除します。

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。この結果、既存のデータが失われることがあります。

ステップ 12 [Next] をクリックします。

ステップ 13 [Physical Drive Configuration] ページで、次のように入力します。

ステップ 14 [Configure Unused Disks] チェックボックスをオンにし、未使用ディスクを [Unconfigured Good] または [JBOD] 状態に設定するオプションを選択します。

（注） [Unconfigured Good] を選択すると、[Clear Secure Drive] チェックボックスが表示されます。[JBOD] を選択すると、[Enable Secure Drive] チェックボックスが表示されます。

ステップ 15 物理ドライブ上のすべてのデータを削除する場合は [Clear Secure Drive] チェックボックスをオンにし、セキュア ドライブを有効にする場合は [Enable Secure Drive] チェックボックスをオンにします。

ステップ 16 [送信（Submit）] 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。ホスト コンソールへCisco IMC Supervisorを使用して到達する場合は、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] を選択したら、[Add] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [Add] 画面で、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] ウィンドウが表示されます。既存の設定からのポリシーの作成 （38 ページ）を参照してください。

ステップ 4 Cisco UCS S3260 サーバ用のポリシーの場合は、[Cisco UCS S3260] 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 5 [Main] ウィンドウで、[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 6 [送信（Submit）] をクリックします。

SNMP ポリシー

Cisco IMC Supervisor は、Simple Network Management Protocol（SNMP）設定、および管理対象サーバから SNMP トラップによって障害およびアラート情報を送信するための設定をサポートします。

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] を選択したら、[Add] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [Add] 画面で、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] ウィンドウが表示されます。既存の設定からのポリシーの作成 （38 ページ）を参照してください。

ステップ 4 Cisco UCS S3260 サーバ用のポリシーの場合は、[Cisco UCS S3260] 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 5 [SNMP Users] ウィンドウで [+] 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。

（注） **DES** プライバシー タイプは、CIMC バージョン 4.1（3b）および Cisco IMC Supervisor バージョン 2.3 ではサポートされていません。

ステップ 6 [Next] をクリックします。

ステップ 7 [SNMP Traps] ウィンドウで [+] 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 8 [Next] をクリックします。

ステップ 9 [SNMP Settings] ウィンドウで、SNMP プロパティを設定します。

ステップ 10 [Submit] 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 **SNMP ポート**を設定することはできません。該当するサーバではチェックボックスを使用して除外する必要があります。
- バージョン 2.x の Cisco IMC を実行している E シリーズ サーバで **SNMP ポート**を設定することはできません。該当するサーバではチェックボックスを使用して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] を選択したら、[Add] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [Add] ウィンドウで、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] ウィンドウが表示されます。既存の設定からのポリシーの作成 （38 ページ）を参照してください。

ステップ 4 Cisco UCS S3260 サーバ用のポリシーの場合は、[Cisco UCS S3260] 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 5 [Main] ウィンドウで [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 6 [送信（Submit）] をクリックします。

ユーザ ポリシー

ユーザ ポリシーを使用して、ローカル ユーザの設定を自動化できます。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。

各種プロパティの設定に関する詳細は、『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] を選択したら、[Add] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [Add] ウィンドウで、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] ウィンドウが表示されます。既存の設定からのポリシーの作成 （38 ページ）を参照してください。

ステップ 4 Cisco UCS S3260 サーバ用のポリシーの場合は、[Cisco UCS S3260] 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 5 [Main] ウィンドウで、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 6 次のステップで設定するユーザに強力なパスワードを適用する場合は、[Enforce Strong Password] チェックボックスをオンにします。

この機能は、CIMC 2.0(9c) 以上を実行しているサーバにのみ適用できます。

ステップ 7 [+] をクリックして、ユーザを追加します。

ステップ 8 [Add Entry to Users] ウィンドウで、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。
ロール（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。
[Enable User Account]	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。
[新しいパスワード（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。
新しいパスワードの確認	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 9 [Submit] をクリックします。

ステップ 10 パスワードの有効期限ポリシーを適用するには、[Add Password Expiration Policy] チェックボックスをオンにします。

（注） パスワードの有効期限ポリシーを個別に適用できません。

ステップ 11 ドロップダウン リストから既存のパスワードの有効期限ポリシーを選択するか、[+] をクリックして新しいパスワードの有効期限ポリシーを追加します。パスワードの有効期限ポリシー（22 ページ）を参照してください。

ステップ 12 [Submit] をクリックします。

また、[Main] ウィンドウの [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。
- 2.0(8d) より古いバージョンの CIMC を実行しているサーバの場合、Cisco IMC Supervisorにより、ポリシーで定義されているものとともに、サーバにダミーのユーザー エントリが作成されています。CIMC 2.0(8d) 以上を実行しているサーバにポリシーを適用する場合、ブランク ユーザ エントリは作成されません。（以前のポリシーにより適用された）既存のダミー ユーザ エントリはクリアされます。
- Cisco IMC Supervisor の管理に使用されるアカウントが、ポリシーのユーザー リストから削除されていないことを確認します。削除されている場合、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] を選択したら、[Add] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [Add] ウィンドウで、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] ウィンドウが表示されます。既存の設定からのポリシーの作成 （38 ページ）を参照してください。

ステップ 4 Cisco UCS S3260 サーバ用のポリシーの場合は、[Cisco UCS S3260] 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 5 [Enable vKVM] チェックボックスをオンにします。

ステップ 6 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 7 [送信（Submit）] をクリックします。

VIC アダプタ ポリシー

さまざまな VIC アダプタ プロパティの設定の詳細については、Cisco UCS C シリーズ サーバの統合管理コントローラ GUI の構成ガイド（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。

手順

ステップ 1 [Hardware Policies] を選択したら、[Add] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [Add] 画面で、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] 画面が表示されます。既存の設定からのポリシーの作成 （38 ページ）を参照してください。

ステップ 4 Cisco UCS S3260 サーバ用のポリシーの場合は、[Cisco UCS S3260] 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 5 [Main] 画面で [+] 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 6 **[VIC アダプタにエントリを追加 (Add Entry TO VIC Adapters)]** 画面で、次のアダプタの詳細を編集するか、確認することができます。

- **PCI スロット選択**：アダプタを使用可能な PCI スロットまたは特定の PCI スロットに装着するかを指定します。[任意 (Any)] を選択すると、**[PCI スロット (PCI Slot)]** フィールドは表示されません。
- **PCI スロット**：アダプタが装着されている PCI スロット。
- **説明**：アダプタの説明
- **FIP モード**：FCoE Initialization PROTOCOL (FIP) モードを有効にするか無効にするかを指定します。
- **LLDP の設定**：オンにすると、Link Layer Discovery Protocol（LLDP）によってすべての Data Center Bridging Capability Exchange プロトコル（DCBX）機能が有効になります。これには、FCoE、プライオリティ ベースのフロー制御も含まれます。18-06-2020 18:12
- **Vntag モード**：VNTAG モードを有効にするか無効にするかを指定します。
- **ポート チャネル**：ポートチャネルを **[有効 (Enabled)]**、**[無効 (Disabled)]**、または **[適用されない (Not Applicable)]** 状態に設定します。Cisco VIC 1455 および 1457 アダプタの場合、

ポート チャネルはデフォルトで **[有効 (Enabled)]** に設定されています。ポート チャネル設定をサポートしていないアダプタの場合、このフィールドは **[適用されない (Not Applicable)]** に設定されます。vNICs と Vnics は、このフィールドで選択されたポート チャネルの状態に基づいて、デフォルトで設定されます。ポートチャネルの状態を変更すると、既存の設定が最新の設定に上書きされます。**[ポート チャネル (Port Channel)]** フィールドが **[有効 (Enabled)]** または **[適用しない (Not Applicable)]** に設定されている場合、デフォルトで少なくとも 2 個の vNIC (eth0 と Eth1) と 2 個の vHBA (fc0 と fc1) が設定されます。**[ポート チャネル (Port Channel)]** フィールドが **[無効 (Disabled)]** に設定されている場合、最低 4 個の vNIC (eth0、eth1、eth2、および eth3) と 4 個の vhba (fc0、fc1、fc2、および fc3) がデフォルトで設定されます。ただし、これらのアダプタに追加の vHBA または vNIC を作成できます。

- **外部イーサネット インターフェイス**: Cisco VIC 1455、Cisco VIC 1457、Cisco VIC 1495、Cisco VIC 1497 アダプタの管理前方誤り訂正 (FEC) モードを設定します。デフォルトでは、4 個のポートがあり、削除することはできません。ただし、[管理 FEC (Admin FEC)] モードで設定されたポート数は、選択したアダプタに基づきます。たとえば、Cisco VIC 1497 アダプタでは 2 ポートのみです。したがって、[管理 FEC (Admin FEC)] モードは最初の 2 ポート (ポート 0 およびポート 1) でのみ設定されており、残りのポート (ポート 2 およびポート 3) は無視されます。

  既存のポリシーでは、このフィールドは **[自動（Auto）]** に設定されています。しかし、値を **cl91**、**cl74**、**Off** に変更できます。アダプタ モデルが [管理 FEC (Admin FEC)] モードをサポートしていない場合、これらの値は無視されます。

  （注） **cl74**オプションは、Cisco VIC 1495 および Cisco VIC 1497 アダプタではサポートされていません。

- **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。**[ポート チャネル (Port Channel)]** フィールドが **[有効 (Enabled)]** または **[適用しない (Not Applicable)]** に設定されている場合、デフォルトでは 2 個以上の vNIC (eth0 と eth1) が設定され、アップリンク ポートは 0 および 1 となります。**[ポート チャネル (Port Channel)]** フィールドが **[無効 (Disabled)]** に設定されている場合、デフォルトで 0 ~ 3 のアップリンク ポートを使用して、最低 4 個の vNIC、eth0、eth1、eth2、および eth3 が設定されます。ただし、これらのアダプタに追加の vNIC を作成できます。

- **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。**[ポート チャネル (Port Channel)]** フィールドが **[有効 (Enabled)]** または **[適用しない (Not Applicable)]** に設定されている場合、デフォルトで少なくとも 2 個の vHBA (fc0 と fc1) が設定されます。**[ポート チャネル (Port Channel)]** フィールドが **[無効 (Disabled)]** に設定されている場合、最低 4 個の vHBA、fc0、fc1、fc2、および fc3 がデフォルトで設定されます。ただし、これらのアダプタに追加の vHBA を作成できます。

ステップ 7 [送信（Submit）] 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、ISO ファイル（CDD を使用）と IMG ファイル（HDD を使用）でそれぞれ 1 つずつ、最大 2 つの vMedia マッピングを設定できます。

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] を選択したら、[Add] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [Add] 画面で、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] ウィンドウが表示されます。既存の設定からのポリシーの作成 （38 ページ）を参照してください。

ステップ 4 Cisco UCS S3260 サーバ用のポリシーの場合は、[Cisco UCS S3260] 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 5 [Main] ウィンドウで、[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 6 [Next] をクリックします。

ステップ 7 [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 8 [Next] をクリックします。

ステップ 9 **[Add HDD vMedia Mapping (HDD vMedia マッピングの追加)** 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 10 [送信（Submit）] をクリックします。

（注）
- 現在、Cisco IMC Supervisor で **[Low Power USB State (低電力 USB 状態)]** を設定することはできません。
- 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。

ゾーン分割ポリシー

ゾーン分割ポリシーは、サーバに物理ドライブを割り当てるために使用されます。Cisco UCS S3260 高密度ストレージ ラック サーバは、Cisco Management Controller（CMC）の Serial Attached SCSI（SAS）ドライブのダイナミック ストレージをサポートしています。このダイナミック ストレージのサポートは、CMC の SAS Fabric Manager によって提供されます。ダイナミック ストレージは次のオプションをサポートしています。

- サーバ 1 およびサーバ 2 への物理ディスクの割り当て
- シャーシ幅ホット スペア（RAID コントローラでのみサポート）
- 共有モード（HBA でのみサポート）
- 物理ディスクの割り当て解除
- SAS エクスパンダ プロパティの表示
- サーバへの物理ドライブの割り当て
- シャーシ幅ホット スペアとしての物理ドライブの移動
- 物理ドライブの割り当て解除
- 選択した物理ドライブを割り当てるコントローラ スロットを選択できます。

ディスク グループの各種プロパティの設定の詳細については、『Cisco UCS C-Series Integrated Management Controller GUI Configuration Guide for S3260 Servers』の「*Dynamic Storage*」の項を参照してください。

ゾーン分割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] を選択したら、[Add] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 ページ）を参照してください。

ステップ 2 [Add] 画面で、ドロップダウン リストから [Zoning 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] ウィンドウが表示されます。既存の設定からのポリシーの作成 （38 ページ）を参照してください。

（注） ゾーン分割ポリシーは Cisco UCS 3260 ラック サーバにのみ適用でき、UI の [Cisco UCS S3260] チェックボックスがデフォルトでオンになっています。

ステップ 4 **[Zoning (ゾーニング)]** ウィンドウで **[+]** をクリックして、サーバ上に設定するローカル ディスクを追加します。

ステップ 5 **[Add Entry to Local Disks (エントリをローカル ディスクに追加)]**ウィンドウで、ローカル ディスクが存在する **[Slot Number (スロット番号)]** を入力します。

ステップ 6 **[Ownership (所有権)]** ドロップダウンリストから、ローカル ディスクの所有権を特定のサーバに割り当てます。

ステップ 7 **[Choose controller (コントローラの選択)]** チェックボックスをオンにして、サーバ内の特定のコントローラにローカル ディスクを割り当てます。

ローカル ディスクのコントローラ スロットの選択は必須ではありません。特定のコントローラ スロットを選択しない場合、ゾーン分割ポリシーは、選択したサーバで使用可能な最初のコントローラ スロットに適用されます。

ステップ 8 **[Controller (コントローラ)]**ドロップダウンリストから、サーバの特定のコントローラ名を選択します。

ステップ 9 あるサーバが所有するディスクを別のサーバに割り当てる場合は、[Force]チェックボックスをオンにします。

ステップ 10 [送信（Submit）] をクリックします。

ステップ 11 ポリシーを設定するには、**[Zoning (ゾーン分割)]** ページで、**[Modify Physical Drive Power Policy (物理ドライブ電源ポリシーの変更)]** チェックボックスをオンにします。

ステップ 12 [Physical Drive Power State] ドロップダウンリストから電源の状態を選択します。

ステップ 13 [送信（Submit）] をクリックします。

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] を選択したら、[Add] をクリックします。このページへのアクセスについては、「ハードウェア ポリシーの作成」（81 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 (サーバの詳細)]** 画面で、次のいずれかの方法でサーバの詳細を指定します。

（注） Cisco UCS S3260 サーバのポリシーを作成している場合は、手順 5 に進みます。

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] 画面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] 画面に進みます。ポリシーの作成を続けます。

ステップ 5 Cisco UCS S3260 サーバの場合は、[Create policy from current configuration of the server] および [Cisco UCS S3260] チェックボックスの両方をオンにして、[Next] をクリックします。

注目 Cisco UCS S3260 サーバでは電力復元ポリシーを作成できません。このポリシーは E シリーズ サーバでのみ作成できます。

ステップ 6 [Server Details] 画面で [Enter Server Details Manually] チェックボックスをオンにして、以下のフィールドに入力するか、または [Select] をクリックして、ポリシーを適用する Cisco UCS S3260 サーバを選択します。

1. Cisco UCS S3260 プラットフォームの [Server IP] フィールドに仮想的な管理 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。

ステップ 7 [Server Node 1] または [Server Node 2] のオプション ボタンを選択します。

ステップ 8 [Next] をクリックします。

[Main] 画面に進みます。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 **[Policies]** > **[Manage Policies and Profiles]** を選択します。

ステップ 2 [Manage Policies and Profiles] ページで、[Hardware Policies] をクリックします。

ステップ 3 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。
[Apply Policy] 画面で、ポリシーを適用する [Chassis] または [Server(s)] を選択できます。これらのオプションは、選択したユーザ管理ポリシーまたはコンピューティング ノード ポリシーに基づいて表示されます。

ステップ 5 [Select] をクリックして、ポリシーを適用するシャーシまたはサーバを選択します。

（注） **[Select (選択)]** で、C シリーズ サーバ (Cisco UCS 3260 サーバを除く)、E シリーズ サーバ、ENCS サーバなどのすべてのサーバが表示されます。電源ポリシーを適用している場合、ENCS サーバはグレー表示され、これらのサーバを選択することはできません。Cisco UCS 3260 サーバの電源ポリシーを作成している場合は、[Select (選択)] をクリックすると、Cisco UCS 3260 サーバのみが表示されます。他のサーバは表示されません。

Cisco UCS 3260 タイプのポリシーの場合、シャーシは管理ポリシーとして、サーバはコンピューティング ノード ポリシーとして表示されます。ポリシーとプロファイル を参照してください。

ステップ 6 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 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。

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 **[Policies]** > **[Manage Policies and Profiles]** を選択します。

ステップ 2 [Manage Policies and Profiles] ページで、[Hardware Policies] をクリックします。

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 （40 ページ）を参照してください。

ステップ 5 状況に応じて、[送信（Submit）] または [閉じる（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。

Cisco IMC Supervisor でハードウェア プロファイルを使用する方法を次のワークフローで説明します。

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。
    1. 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 （42 ページ）を参照してください。
    2. 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（43 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 （45 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。
    1. Edit
    2. 削除
    3. 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 （46 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

手順

ステップ 1 **[Policies]** > **[Manage Policies and Profiles]** を選択します。

ステップ 2 [Manage Policies and Profiles] ページで、[Hardware Profiles] をクリックします。

ステップ 3 [Add] をクリックします。

ステップ 4 [Hardware Profile] 画面で、作成するプロファイルの名前を [Profile Name] フィールドに入力します。

既存のサーバ構成を使用する場合は、[Create profile from current configuration of the server] チェックボックスをオンにすることもできます。これにより、[Server Details] 画面が表示されます。「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 5 Cisco UCS S3260 サーバ用のプロファイルの場合は、[Cisco UCS S3260] 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 6 [Profile Entities] ウィンドウで [+] をクリックして、プロファイル エントリを追加します。

[Delete] アイコンをクリックして、既存のエントリを削除することもできます。

ステップ 7 [Add Entry to Profile Name] ウィンドウで、[Policy Type] を選択します。

ステップ 8 作成済みのポリシーの名前が一覧表示される [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、選択したポリシー タイプに基づき新しいポリシーを作成できます。「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 9 [Apply Policy To] ドロップダウンリストからポリシーを適用するサーバを選択します。

ステップ 10 [Submit] をクリックします。

次のタスク

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できます。ハードウェア プロファイルでの一般タスク （46 ページ） を参照してください

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 **[Policies]** > **[Manage Policies and Profiles]** を選択します。

ステップ 2 [Manage Policies and Profiles] ページで、[Hardware Profiles] をクリックします。

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情報を使用できます。Cisco UCS S3260 サーバの場合はステップ 10 に進みます。

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] ウィンドウで [+] 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 Cisco UCS S3260 サーバの場合は、[Cisco UCS S3260] チェックボックスをオンにして、[Next] をクリックします。

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. Cisco UCS S3260 プラットフォームの [Server IP] フィールドに仮想的な管理 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、サーバから作成するポリシーを選択して、[Select] をクリックします。

ステップ 10 [Next] をクリックします。

ステップ 11 [Profile Entities] ウィンドウで [+] 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。

（注） Cisco UCS S3260 のプロファイル タイプの場合、プラットフォーム タイプが Cisco UCS S3260 のポリシーのみ追加できます。ポリシーがコンピューティング ノード タイプの場合、[Apply Policy To] フィールドでサーバ ノードを指定する必要があります。例、[Server-1]、[Server-2]、および [Both]。管理ポリシーの場合、このフィールドは関係ありません。

ステップ 12 [送信（Submit）] 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 **[Policies]** > **[Manage Policies and Profiles]** を選択します。

ステップ 2 [Manage Policies and Profiles] ページで、[Hardware Profiles] をクリックします。

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。
[Apply Profile] 画面で、プロファイルの適用先として [Chassis]（Cisco UCS S3260 タイプのプロファイルに適用可能）または [Server(s)] を選択できます。これらのオプションを選択したサーバ プラットフォームに基づいて表示されます。

ステップ 4 [Apply Profile] ダイアログボックスで、[Select] をクリックしてプロファイルを適用するシャーシまたはサーバを選択します。

ステップ 5 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 6 [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 7 [Submit] 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 **[Policies]** > **[Manage Policies and Profiles]** を選択します。

ステップ 2 [Manage Policies and Profiles] ページで、[Hardware Profiles] をクリックします。

ステップ 3 [Hardware Profile] を展開し、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。[送信（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。ハードウェア プロファイルの適用 （45 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 4 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 **[Policies]** > **[Tag Library]** を選択します。

ステップ 2 [作成（Create）] をクリックします。

ステップ 3 **[Create Tag (タグの作成)]** 画面で、**[Tag Details (タグの詳細)]** 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]** • **管理（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、セットになったタグ付け可能なエンティティ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 [送信（Submit）] 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。

REST API とオーケストレーション

[REST API Browser (REST API ブラウザ)] 画面には、Cisco IMC Supervisor で提供されておりユーザーが使用できる API のリストが表示されます。API は次のグループに分類されます。

- ファームウェア管理のタスク
- 一般的な作業
- プラットフォーム タスク
- ポリシー タスク
- ポリシーおよびプロファイルのタスク

- サーバー タスク
- ユーザー タスクとグループ タスク

次の操作を実行するには、画面上のコントロールを使用できます。

- リスト全体の展開と折りたたみ
- この画面を **[Favorites (お気に入り)]** に追加する
- **[Search (検索)]** または **[Advanced Filter (高度なフィルタ)]** オプションを使用した特定の API の検出
- レポートのエクスポート
- 管理対象サーバの追加

これらの API の使用法の詳細については、『*Cisco IMC Supervisor REST API Cookbook*』を参照してください。この資料は http://www.cisco.com/c/en/us/support/servers-unified-computing/integrated-management-controller-imc-supervisor/products-programming-reference-guides-list.html から入手できます。