Cisco UCS サーバ プールとポリシーの設定

この章は、次の項で構成されています。

- グローバル機器ポリシー，1 ページ
- UUID プール，4 ページ
- サーバ プール，6 ページ
- 管理 IP プール，9 ページ
- ブート ポリシー，10 ページ
- ローカル ディスク設定ポリシー，61 ページ
- メンテナンス ポリシー，67 ページ
- サーバ プール ポリシー資格情報の概要，70 ページ
- サーバ プール ポリシーの概要，75 ページ
- vNIC/vHBA 配置ポリシー，76 ページ
- 配置ポリシー，84 ページ

グローバル機器ポリシー

シャーシ/FEX 検出ポリシー

シャーシ/FEX 検出ポリシーは、新しいシャーシまたは FEX を追加したときのシステムの対処方法を決定します。Cisco UCS は、シャーシ/FEX ディスカバリ ポリシーの設定を使用して、次の決定を行います。

- シャーシまたは FEX とファブリック インターコネクト間のリンク数の最小しきい値
- IOM からファブリック ポート チャネルのファブリック インターコネクトへのリンクをグループ化するかどうか

シャーシ/FEX検出ポリシーのマルチシャーシCisco UCSドメインでの動作方法の概要を含むシャーシ リンクの詳細については、『Cisco UCS Manager configuration guides』を参照してください。

シャーシ/FEX 検出ポリシーの設定

シャーシ ポリシーの設定では、新しいシャーシを追加したときのシステムの対応方法を指定します。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [機器のグローバル ポリシー（Equipment Global Policies）] をクリックします。

ステップ 4 [シャーシ/FEX検出ポリシー（Chassis/FEX Discovery Policy）] チェックボックスをオンにします。

ステップ 5 [アクション（Action）] ドロップダウン リストで、シャーシまたはファブリック エクステンダ（FEX）とファブリック インターコネクト間のリンク数の最小しきい値を選択します。

- [1-link]
- [2-link]
- [4-link]
- [8-link]

ステップ 6 [リンク グループのプリファレンス（Link Grouping Preference）] ドロップダウン リストから、IOM または FEX からファブリック インターコネクトへのリンクを 1 つのポート チャネルにグループ化するかどうかを選択します。

（注） リンク グループのプリファレンスは、IOM または FEX とファブリック インターコネクトとの間のリンクの両側が、ファブリック ポート チャネルをサポートしている場合にのみ有効になります。リンクの一方がファブリック ポート チャネルをサポートしていない場合は、このプリファレンスは無視され、リンクはポート チャネルにグループ化されません。

ステップ 7 [保存（Save）] をクリックします。

ラック サーバ ディスカバリ ポリシー

ラック サーバ ディスカバリ ポリシーは、新しいラックマウント サーバを追加したときのシステムの対処方法を決定します。Cisco UCS は、ラック サーバ ディスカバリ ポリシーの設定を使用して、ハード ディスク上のデータをスクラビングするかどうか、サーバ検出をただちに開始するかユーザの明示的な確認応答を待つ必要があるかを決定します。手動の確認応答については、Cisco UCS Manager の保留アクティビティ レポートの表示とユーザの確認応答 を参照してください。

Cisco UCS は、ファブリック インターコネクトに適切にケーブル接続されていないラックマウント サーバを検出できません。サポートされる Cisco UCS ラックマウント サーバの統合方法については、適切な『rack-mount server integration guide』を参照してください。

ラック サーバ ディスカバリ ポリシーの設定

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [機器のグローバル ポリシー（Equipment Global Policies）] をクリックします。

ステップ 4 [ラックサーバ検出ポリシー（Rack Server Discovery Policy）] チェックボックスをオンにします。

ステップ 5 [アクション（Action）] ドロップダウン リストから、新しいラック サーバを追加する際のアクションを選択します。

- [即時（Immediate）]：新しいサーバが自動的に検出されます。
- [ユーザ承認済み（User-acknowledged）]：ユーザが新しいサーバを承認するまで、何も起こりません。

  ユーザの確認応答を適用するには、Cisco UCS Manager の保留アクティビティ レポートの表示とユーザの確認応答 を参照してください。

ステップ 6 [スクラビングポリシー（Scrub Policy）] ドロップダウン リストから、サーバがサーバ プールのポリシー資格情報の条件を満たした場合に、新しく検出されたサーバで実行されるスクラビング ポリシーを選択します。

ステップ 7 [保存（Save）] をクリックします。

ラック管理接続ポリシー

ラック管理接続ポリシーは、新しく追加されたラックマウント サーバが Cisco UCS によって自動的に管理されるかユーザの明示的な承認を待機する必要があるかを決定します。自動的に承認されるようにこのポリシーを設定することをお勧めします。

ラック管理接続ポリシーの設定

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [機器のグローバル ポリシー（Equipment Global Policies）] をクリックします。

ステップ 4 [ラックサーバディスカバリポリシー（Rack Management Connection Policy）] チェックボックスをオンにします。

ステップ 5 [アクション（Action）] ドロップダウン リストから、次のいずれかを選択します。

- [自動確認応答（auto-acknowledged）]：確認応答が自動的に実行されます。
- [ユーザ承認済み（user-acknowledged）]：ユーザがサーバを承認するまで、何も起こりません。

  ユーザの確認応答を適用するには、Cisco UCS Manager の保留アクティビティ レポートの表示とユーザの確認応答 を参照してください。

ステップ 6 [保存（Save）] をクリックします。

UUID プール

UUID プールは、サーバに割り当てることができる SMBIOS（オペレーティング システム上に構築されるシステム管理）UUID（汎用一意識別子）のコレクションです。UUID の接頭辞を構成する先頭の桁の数字は固定されています。残りの桁で構成される UUID 接尾辞は変数です。UUID プールは、特定のプールを使用するサービス プロファイルに関連づけられた各サーバについて、これらの変数が一意であることを保証して競合を回避します。

サービス プロファイルで UUID プールを使用する場合、サービス プロファイルに関連付けられたサーバの UUID を手動で設定する必要はありません。

UUID プールの作成

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 プールを作成する組織をクリックし、[詳細の表示（View Details）] をクリックします。

ステップ 5 [UUID プール（UUID Pools）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [UUID プールの追加（Add UUID Pool）] 画面で、次のフィールドに値を入力します。

名前	説明
[名前（Name）] フィールド	プールの一意の名前。
[説明（Description）] フィールド	プールの説明。
[プレフィックス（Prefix）] ドロップダウン リスト	プレフィックスの作成方法を選択します。次のいずれかになります。 • [派生（Derived）] : システムによってプレフィックスが作成されます。 • [その他（Other）] : 任意のプレフィックスを指定します。 このオプションを選択すると、任意のプレフィックスを XXXXXXXX-XXXX-XXXX の形式で入力できるテキスト フィールドが表示されます。
[開始（Other）] フィールド	ブロック内の最初の UUID アドレス。
[サイズ（Size）] フィールド	ブロック内の UUID アドレスの数。

ステップ 8 [送信（Submit）] をクリックします。

UUID プールへのアドレス ブロックの追加

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 プールを変更する組織をクリックし、[詳細の表示（View Details）] をクリックします。

ステップ 5 [UUID プール（UUID Pools）] をクリックします。

ステップ 6 アドレスブロックを追加するプールをクリックして、[UUIDアドレスブロックの追加（Add UUID Addresses Block）] をクリックします。

ステップ 7 [UUID プール ブロックの追加（Add UUID Pool Block）] 画面で、次のフィールドに値を入力します。

名前	説明
[開始（From）] フィールド	ブロック内の最初の UUID アドレス。
[サイズ（Size）] フィールド	ブロック内の UUID アドレスの数。

ステップ 8 [送信（Submit）] をクリックします。

サーバ プール

サーバ プールは複数のサーバで構成されています。これらのサーバは通常、同じ特性を持っています。これらの特性は、シャーシ内の位置であったり、サーバタイプ、メモリ容量、ローカルストレージ、CPU のタイプ、ローカル ドライブ設定などの属性だったりします。サーバを手動でサーバ プールに割り当てることも、サーバ プール ポリシーとサーバ プール ポリシー資格情報を使用して割り当てを自動化することもできます。

システムが組織を通じて、マルチテナント機能を実装している場合、特定の組織で使用されるサーバ プールを 1 つ以上、指定できます。たとえば、CPU を 2 個搭載したサーバをすべて含むプールをマーケティング組織に割り当て、メモリのサイズが 64GB のサーバをすべて、財務組織に割り当てることができます。

サーバ プールには、システム内のどのシャーシにあるサーバでも入れることができます。1 つのサーバは複数のサーバ プールに属することができます。

サーバ プールの作成

Cisco UCS Director では、サーバ プールのマネージド サーバのみが表示されますが、プールのサイズにはすべてのサーバが含まれます。たとえば、サーバ プールに 2 台のサーバがあり、そのうち 1 台のサーバのみが Cisco UCS Director で管理されている場合、そのプールのすべてのサーバ プール レポートとアクションには、1 台の（マネージド）サーバのみが表示されます。ただし、プール サイズは 2 台と表示されます。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 プールを作成する組織をクリックし、[詳細の表示（View Details）] をクリックします。

ステップ 5 [サーバ プール（Server Pools）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [サーバ プールの追加（Add Server Pool）] 画面に、プールの名前と説明を入力します。

ステップ 8 （任意） [サーバ（Servers）] フィールドで、次の手順を実行してプールにサーバを追加します。

a) [選択（Select）] をクリックします。

b) [項目の選択（Select Items）] ページで、プールに追加するサーバのチェックボックスをオンにします。

c) [選択（Select）] をクリックします。

ステップ 9 [追加（Add）] をクリックします。

Cisco UCS Director グループへのサーバ プールの割り当て

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 割り当てるプールのある組織をクリックし、[詳細の表示（View Details）] をクリックします。

ステップ 5 [サーバ プール（Server Pools）] をクリックします。

ステップ 6 Cisco UCS Director グループに割り当てるプールの表の列をクリックします。

ステップ 7 [グループの割り当て（Assign Group）] をクリックします。

ステップ 8 [グループの選択（Select Group）] 画面で、次の手順を実行します。

a) [グループ（Group）] ドロップダウン リストから、Cisco UCS Directorサーバ プールを割り当てるグループを選択します。

b) [ラベル（Label）] フィールドに、サーバ プールを示すラベルを入力します。

c) [送信（Submit）] をクリックします。

Cisco UCS Director グループからのサーバ プロファイルの割り当て解除

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 割り当て解除するプールが含まれている組織をクリックし、[詳細の表示（View Details）] をクリックします。

ステップ 5 [サーバ プール（Server Pools）] をクリックします。

ステップ 6 [サーバ プール（Server Pool）] ページで、Cisco UCS Director グループから割り当てを解除するプールの行をクリックし、[詳細の表示（View Details）] をクリックします。

ステップ 7 [UCS サーバ（UCS Servers）] をクリックします。

ステップ 8 割り当てを解除するサーバの行をクリックします。

ステップ 9 [その他のアクション（More Actions）] ドロップダウン メニューから、[グループの割り当て解除（Unassign Group）] を選択します。

ステップ 10 [グループの割り当て解除（Unassign Group）] 画面で、[割り当て解除（Unassign）] をクリックします。

管理 IP プール

管理 IP プールは外部 IP アドレスの集合です。管理 IP プール内の IP アドレスの各ブロックは、サーバ上の CIMC（Cisco Integrated Management Controller）で終了する外部アクセス用に予約されています。

管理 IP プールのすべての IP アドレスは、ファブリック インターコネクトの IP アドレスと同じサブネット内にあることが必要です。

（注） サーバまたはサービス プロファイルのスタティック IP アドレスとして割り当てられている IP アドレスが、管理 IP プールに含まれていてはなりません。

管理 IP プールへの IP アドレス ブロックの追加

サーバまたはサービス プロファイルのスタティック IP アドレスとして割り当てられている IP アドレスが、管理 IP プールに含まれていてはなりません。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [管理 IP プール（Management IP Pool）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [IP アドレスのブロックの作成（Create Block of IP Addresses）] 画面で、次のフィールドに値を入力します。

名前	説明
[開始（From）] フィールド	ブロック内の最初の IP アドレス。
[サイズ（Size）] フィールド	プール内の IP アドレスの数。
[サブネット マスク（Subnet Mask）] フィールド	ブロック内の IP アドレスに関連付けられたサブネット マスク。これは、ファブリック インターコネクトと同じサブネットマスクである必要があります。
[デフォルト ゲートウェイ（Default Gateway）] フィールド	ブロック内の IP アドレスに関連付けられたデフォルト ゲートウェイ。

ステップ 6 [送信（Submit）] をクリックします。

ブート ポリシー

Cisco UCS Manager を使用して、ブレード サーバ、ラック サーバ、およびモジュラ サーバのブート ポリシーを作成することができます。

Cisco UCS Manager ブート ポリシーは、BIOS 設定メニューのブート順序をオーバーライドし、次のことを決定します。

- ブート デバイスの選択
- サーバのブート元である場所
- ブート デバイスの起動順序

たとえば、関連するサーバをローカル ディスクや CD-ROM（VMedia）などのローカル デバイスから起動したり、SAN ブートや LAN（PXE）ブートを選択することができます。

1 つ以上のサービス プロファイルに関連付ける名前付きブート ポリシーを作成するか、または特定のサービス プロファイルに対するブート ポリシーを作成できます。ブート ポリシーを有効にするには、ブート ポリシーをサービス プロファイルに含め、このサービス プロファイルをサーバに関連付ける必要があります。サービス プロファイルにブート ポリシーを含めない場合、Cisco UCS Manager によってデフォルトのブート ポリシーが適用されます。

（注） ブート ポリシーに対する変更は、そのブート ポリシーを含んでいる、更新中のサービス プロファイル テンプレートを使って作成されたすべてのサーバに伝播されます。BIOS にブート順序情報を再書き込みするためのサービス プロファイルとサーバとの再関連付けは自動的にトリガーされます。

また、ブート ポリシーに次の内容を指定することもできます。

- ローカル LUN の名前。指定された名前は、展開される名前ではなく、ストレージ プロファイル内の論理名です。モジュラ サーバの場合、プライマリ名とセカンダリ名の両方を指定できます。他のサーバの場合は、プライマリ名のみを指定します。セカンダリ名を指定すると、設定エラーが発生します。
- JBODディスクからブートするための特定のJBODディスク番号。これは、モジュラ サーバではサポートされません。
- 下位互換性のための任意の LUN。ただし、これは非推奨です。その他のデバイスを正常にブートさせるには、ブート可能なイメージを保持していない必要があります。

UEFI ブート モード

Unified Extensible Firmware Interface（UEFI）は、オペレーティング システムとプラットフォーム ファームウェア間のソフトウェア インターフェイスを定義する仕様です。Cisco UCS Manager は、UEFI を使用して BIOS ファームウェア インターフェイスを置換します。これにより、BIOS は UEFI モードで動作すると同時に、レガシーもサポートできます。

ブート ポリシーを作成する場合、レガシー ブート モードまたは UEFI ブート モードのいずれかを選択できます。レガシー ブート モードはすべての Cisco UCS サーバでサポートされています。UEFI ブート モードは M3 以降のサーバでのみサポートされ、このモードで UEFI セキュア ブート モードを有効にできます。

UEFI PXE ブートは、Cisco UCS Manager リリース 2.2(4) 以降と統合された Cisco UCS ラック サーバ上のすべての Cisco VIC アダプタでサポートされています。Cisco UCS Manager リリース 2.2(1) 以降では、すべての Cisco ブレード サーバで UEFI PXE ブートがサポートされます。

次の制限は、UEFI ブート モードに適用されます。

- UEFI ブート モードは、次の組み合わせではサポートされません。
  - Cisco UCS Manager と統合された Cisco UCS ブレード サーバおよびラック サーバ上の Gen-3 Emulex アダプタおよび QLogic アダプタ。

- Cisco UCS Manager と統合された Cisco UCS ラック サーバ上のすべてのアダプタに対する iSCSI ブート。

- 2 つの iSCSI LUN を使用して UEFI ブート モードを使用する場合は、Cisco UCS Manager による IQN サフィックス プールからの名前の選択を許可するのではなく、共通の iSCSI イニシエータ名を基盤となっている iSCSI eNIC の両方に適用されるサービス プロファイルに手動で指定する必要があります。共通の名前を指定しなかった場合は、Cisco UCS Manager は 2 番目の iSCSI LUN を検出できません。
- 同じサーバで UEFI とレガシー ブート モードを混在させることはできません。
- ブート ポリシーに設定されたブート デバイスにインストール済みの UEFI 対応オペレーティング システムがある場合にのみ、サーバは UEFI モードで正しく起動します。互換性のある OS が存在しない場合、ブート デバイスは [ブート順序の詳細（Boot Order Details）] 領域の [実際のブート順序（Actual Boot Order）] タブに表示されません。
- 一部の特殊なケースでは、UEFI ブート マネージャ エントリが BIOS NVRAM に正しく保存されなかったことが原因で、UEFI ブートが失敗することがあります。UEFI シェルを使用して UEFI ブート マネージャ エントリを手動で入力できます。この状況は、以下の場合に発生する可能性があります。
  - UEFI ブート モードがイネーブルになっているブレード サーバとサービス プロファイルの関連付けが解除されており、[機器（Equipment）] タブまたは前面パネルを使用してブレードの電源が手動で投入されている場合。
  - UEFI ブート モードがイネーブルになっているブレード サーバとサービス プロファイルの関連付けが解除されており、ダイレクト VIC ファームウェア アップグレードが試行された場合。
  - UEFI ブート モードがイネーブルになっているブレード サーバまたはラック サーバが SAN LUN でブートオフされ、サービス プロファイルが移行された場合。

Cisco UCS Manager で UEFI ブート パラメータを作成できます。UEFI ブート パラメータ，（13 ページ） 詳細情報を提供します。

UEFI セキュア ブート

Cisco UCS Manager は、Cisco UCS B シリーズ M3 および M4 ブレード サーバ、Cisco UCS C シリーズ M3 および M4 ラック サーバ、および Cisco UCS S シリーズ M4 ラック サーバで UEFI セキュア ブートをサポートしています。UEFIセキュア ブートがイネーブルの場合、すべての実行可能ファイル（ブート ローダ、アダプタ ドライバなど）はロードされる前に BIOS によって認証されます。認証されるには、イメージが Cisco 認証局（CA）または Microsoft CA によって署名される必要があります。

次の制限は、UEFI セキュア ブートに適用されます。

- UEFI ブート モードは、ブート ポリシーでイネーブルにする必要があります。

- Cisco UCS Manager ソフトウェアと BIOS ファームウェアは、リリース 2.2 以上である必要があります。

（注） UEFI ブート モードは、リリース 2.2(3a) 以降の Cisco UCS C シリーズおよび S シリーズ ラック サーバでサポートされます。

- ユーザ生成された暗号キーはサポートされません。
- UEFI セキュア ブートは、Cisco UCS Manager でのみ制御することができます。
- サーバがセキュア ブート モードである場合に Cisco UCS Manager の以前のバージョンにダウングレードする場合で、セキュア ブート モードのシステムがある場合は、ダウングレード前に、サーバの関連付けを解除してから、再度関連付けする必要があります。これを行わないと、サーバは検出されません。

UEFI ブート パラメータ

サーバの UEFI ブート モードは、プラットフォーム ハードウェアに保存されている情報によって決まります。UEFI OS ブート ローダに関する情報を含むブート エントリは、サーバの BIOS フラッシュに保存されます。2.2(4) より前の Cisco UCS Manager リリースでは、サービス プロファイルがあるサーバから別のサーバに移行されると、ブートローダ情報は宛先サーバで使用できなくなります。そのため、BIOS は、サーバを UEFI ブート モードでブートするためのブート ローダ情報をロードできません。

Cisco UCSM リリース 2.2(4) では、宛先サーバ上の UEFI OS ブート ローダの位置に関する情報を BIOS に提供する UEFI ブート パラメータが導入され、BIOS はその位置からブート ローダをロードできます。サーバは、そのブート ローダ情報を使用して、UEFI ブート モードでブートできます。

SAN ブート

SAN 上のオペレーティング システム イメージから 1 つ以上のサーバがブートするように、ブート ポリシーを設定できます。ブート ポリシーにはプライマリとセカンダリの SAN ブート含めることができます。プライマリ ブートが失敗した場合、サーバはセカンダリからのブートを試行します。

システムに最高のサービス プロファイル モビリティを提供する SAN ブートの使用を推奨します。SAN からブートした場合、サービス プロファイルを別のサーバに移動しても、そのサーバは同じオペレーティング システム イメージからブートします。したがって、ネットワークからは、新しいサーバが同じサーバとして認識されます。

SAN ブートを使用するには、次の項目が設定されていることを確認してください。

- Cisco UCS ドメインが、オペレーティング システム イメージをホストしている SAN ストレージ デバイスと通信できること。

- オペレーティング システム イメージが置かれているデバイス上のブート ターゲット LUN（論理ユニット番号）。

（注） SAN ブートは、Cisco UCS ブレード サーバおよびラック サーバ上の Gen-3 Emulex アダプタではサポートされていません。

SAN ブート ポリシーの作成

ヒント ブート ポリシーのブート順序には、ローカル ディスクと SAN LUN の両方ではなく一方のみを組み込み、サーバが誤ったストレージ タイプからブートしないようにすることを推奨します。ローカル ディスクと SAN LUN の両方がブート順序のストレージ タイプに設定されていて、オペレーティング システムまたは論理ボリューム マネージャ（LVM）の設定が誤っている場合、サーバが SAN LUN ではなくローカル ディスクからブートする場合があります。

たとえば、Red Hat Linux がインストールされているサーバで、LVM にデフォルトの LVM が設定されていて、ブート順序に SAN LUN とローカル ディスクが設定されている場合、Linux は同じ名前の LV が 2 つあるという通知を生成し、SCSI ID の値が最も小さい LV（ローカル ディスクの可能性があります）からブートします。

はじめる前に

SAN LUN からサーバをブートするブート ポリシーを作成し、安定した SAN ブート操作が必要な場合は、ブート ポリシーを含むサービス プロファイルに関連付けられたサーバからすべてのローカル ディスクを最初に削除することをお勧めします。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 ポリシーを作成する組織をクリックして [詳細の表示（View Details）] をクリックします。

ステップ 5 [ブート ポリシー（Boot Policies）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [ブート ポリシーの追加（Add Boot Policy）] 画面で、次のフィールドに入力します。

名前	説明
[名前（Name）] フィールド	ポリシーの一意の名前。
[説明（Description）] フィールド	ポリシーの説明。

名前	説明
[順序を変更したときにリブートする（Reboot on Order Change）] チェックボックス	このチェックボックスをオンにすると、ブートの順序を変更した後で、このブートポリシーを使用するすべてのサーバがリブートされます。 このチェックボックスをオンにすると、CD-ROM またはフロッピーがブート順序の最後のデバイスである場合、デバイスの取り外しまたは装着をしても、ブート順には直接効力がないため、サーバはリブートされません。
[vNIC名またはvHBA名の適用（Enforce vNIC/vHBA Name）] チェックボックス	このチェックボックスをオンにすると、ブート順序表に記載されている 1 つ以上の vNIC、vHBA、iSCSI vNIC が、サービス プロファイルのサーバ設定と一致した場合に、設定エラーが表示されます。 オフにした場合、ポリシーはサービスプロファイル内のサーバ設定から vNIC、vHBA、または iSCSI vNIC（ブート オプションに適切なもの）を使用します。ブートポリシーで指定されている vNIC、vHBA、iSCSI vNIC が、サービス プロファイルのサーバ設定と一致するかどうかについてはレポートされません。
[ブート モード（Boot Mode）] ドロップダウンリスト	このブートポリシーを使用するサーバのブートモード。次のいずれかを設定できます。 • [レガシー（Legacy）] • [UEFI] このオプションでは、下位レベルのブートデバイスを指定し、セキュア ブート オプションを有効にできます。
[ブート セキュリティ（Boot Security）] チェックボックス	（ブート モードとして [UEFI] が選択されている場合にのみ表示されます。）このブートポリシーを使用するサーバのセキュア ブート オプションを有効にします。

ステップ 8 [ブート デバイスの追加（Add Boot Device）] 領域で、[SAN ブートの追加（Add SAN Boot）] をオンにして、次のような追加パラメータを入力します。

- [プライマリ vHBA（Primary vHBA）] フィールドに、LAN ブート ロケーションの最初のアドレスとして使用する vHBA 名を入力します。

- [セカンダリ vHBA（Secondary vHBA）] フィールドに、LAN ブート ロケーションの 2 つ目のアドレスとして使用する vHBA 名を入力します。
- プライマリ vHBA とセカンダリ vHBA のいずれかまたは両方がブート可能な SAN イメージをポイントしている場合は、その vHBA の適切な [SAN ブート ターゲットの追加（Add SAN Boot Target）] ボックスをオンにして、次のフィールドに入力します。

名前	説明
[プライマリブートターゲットLUN（Primary Boot Target LUN）] フィールド	ブート イメージの場所に対応する LUN。
[プライマリブートターゲットWWPN（Primary Boot Target WWPN）] フィールド	ブート イメージの場所に対応する WWPN。
[セカンダリブートターゲットLUN（Secondary Boot Target LUN）] フィールド	ブート イメージの場所に対応する LUN。
[セカンダリブートターゲットWWPN（Secondary Boot Target WWPN）] フィールド	ブート イメージの場所に対応する WWPN。

ステップ 9 [iSCSI ブートの追加（Add iSCSI Boot）] をオンにして、次のような追加パラメータを入力します。

- [プライマリ iSCCI vNIC の追加（Add Primary iSCSI vNIC）] フィールドに、ブート ロケーションの最初のアドレスとして使用する iSCSI vNIC 名を入力します。
- [セカンダリ iSCCI vNIC の追加（Add Secondry iSCSI vNIC）] フィールドに、ブート ロケーションの 2 つ目のアドレスとして使用する iSCSI vNIC 名を入力します。

ステップ 10 [送信（Submit）] をクリックします。

LAN ブート

LAN の集中プロビジョニング サーバから 1 つまたは複数のサーバをブートするブート ポリシーを設定できます。LAN（または PXE）ブートは、その LAN サーバからサーバに OS をインストールする際に頻繁に使用されます。

LAN ブート ポリシーには、複数のタイプのブート デバイスを追加できます。たとえば、ローカル ディスクや仮想メディア ブートをセカンダリ ブート デバイスとして追加できます。

LAN ブート ポリシーの作成

ブートポリシーには、複数のタイプのブートデバイスを追加できます。たとえば、ローカルディスク ブートをセカンダリ ブート デバイスとして追加できます。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 ポリシーを作成する組織をクリックして [詳細の表示（View Details）] をクリックします。

ステップ 5 [ブート ポリシー（Boot Policies）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [ブート ポリシーの追加（Add Boot Policy）] 画面で、次のフィールドに入力します。

名前	説明
[名前（Name）] フィールド	ポリシーの一意の名前。
[説明（Description）] フィールド	ポリシーの説明。
[順序を変更したときにリブートする（Reboot on Order Change）] チェックボックス	このチェックボックスをオンにすると、ブートの順序を変更した後で、このブートポリシーを使用するすべてのサーバがリブートされます。 このチェックボックスをオンにすると、CD-ROM またはフロッピーがブート順序の最後のデバイスである場合、デバイスの取り外しまたは装着をしても、ブート順には直接効力がないため、サーバはリブートされません。
[vNIC名またはvHBA名の適用（Enforce vNIC/vHBA Name）] チェックボックス	このチェックボックスをオンにすると、ブート順序表に記載されている 1 つ以上の vNIC、vHBA、iSCSI vNIC が、サービス プロファイルのサーバ設定と一致した場合に、設定エラーが表示されます。 オフにした場合、ポリシーはサービスプロファイル内のサーバ設定から vNIC、vHBA、または iSCSI vNIC（ブート オプションに適切なもの）を使用します。ブートポリシーで指定されている vNIC、vHBA、iSCSI vNIC が、サービス プロファイルのサーバ設定と一致するかどうかについてはレポートされません。

名前	説明
[ブート モード（Boot Mode）] ドロップダウン リスト	このブート ポリシーを使用するサーバのブート モード。次のいずれかを設定できます。 • [レガシー（Legacy）] • [UEFI] このオプションでは、下位レベルのブート デバイスを指定し、セキュア ブート オプションを有効にできます。
[ブート セキュリティ（Boot Security）] チェックボックス	（ブート モードとして [UEFI] が選択されている場合にのみ表示されます。）このブート ポリシーを使用するサーバのセキュア ブート オプションを有効にします。

ステップ 8 [ローカル デバイスの追加（Add Local Device）] 領域で、次のオプションから選択します。

名前	説明
[ローカル ディスクの追加（Add Local Disk）] チェックボックス	ブート ポリシーにローカル ディスクを追加します。
[ローカル LUN の追加（Add Local LUN）] チェックボックス	ローカル LUN をブート順序に追加します。
[SD カードの追加（Add SD Card）] チェックボックス	SD カードをブート順序に追加します。
[内部 USB の追加（Add Internal USB）] チェックボックス	内部 USB をブート順序に追加します。
[外部 USB の追加（Add External USB）] チェックボックス	外部 USB をブート順序に追加します。
[CD ROM の追加（Add CD ROM）] チェックボックス	ブート ポリシーに CD ROM を追加します。
[ローカル CD/DVD の追加（Add Local CD/DVD）] チェックボックス	ローカル CD/DVD をブート順序に追加します。
[リモート CD/DVD の追加（Add Remote CD/DVD）] チェックボックス	リモート CD/DVD をブート ポリシーに追加します。

名前	説明
[フロッピーディスクの追加（Add Floppy Disk）] チェックボックス	フロッピー ディスクをブート ポリシーに追加します。
[ローカル フロッピー ディスクの追加（Add Local Floppy Disk）] チェックボックス	ローカル フロッピー ディスクをブート順序に追加します。
[リモート フロッピー ディスクの追加（Add Remote Floppy Disk）] チェックボックス	リモート フロッピー ディスクをブート順序に追加します。

ステップ 9 [ブート デバイスの追加（Add Boot Device）] 領域で、[LAN ブートの追加（Add LAN Boot）] をオンにして、次のような追加パラメータを入力します。

- [プライマリ vNIC（Primary vNIC）] フィールドに、LAN ブート ロケーションの最初のアドレスとして使用する vNIC 名を入力します。
- [セカンダリ vNIC（Secondary vNIC）] フィールドに、LAN ブート ロケーションの 2 つ目のアドレスとして使用する vNIC 名を入力します。

ステップ 10 [ブート デバイスの追加（Add Boot Device）] 領域で、[iSCSI ブートの追加（Add iSCSI Boot）] をオンにして、次のような追加パラメータを入力します。

- [プライマリ iSCSI vNIC（Primary iSCSI vNIC）] フィールドに、LAN ブート ロケーションに定義された最初のアドレスとして使用する vNIC 名を入力します。
- [セカンダリ iSCSI vNIC（Secondary iSCSI vNIC）] フィールドに、LAN ブート ロケーションに定義された 2 つ目のアドレスとして使用する vNIC 名を入力します。

ステップ 11 [送信（Submit）] をクリックします。

ローカル ディスク ブート

サーバにローカル ドライブがある場合は、ブート ポリシーを設定して、そのデバイスや次のローカル デバイスからサーバをブートできます。

- ローカル ハードディスク ドライブ
- SD カード
- 内蔵 USB
- 外付け USB

ローカル ディスク ブート ポリシーの作成

ブート ポリシーには、複数のタイプのブート デバイスを追加できます。たとえば、ローカル ディスク ブートをセカンダリ ブート デバイスとして追加できます。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 ポリシーを作成する組織をクリックして [詳細の表示（View Details）] をクリックします。

ステップ 5 [ブート ポリシー（Boot Policies）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [ブート ポリシーの追加（Add Boot Policy）] 画面で、次のフィールドに入力します。

名前	説明
[名前（Name）] フィールド	ポリシーの一意の名前。
[説明（Description）] フィールド	ポリシーの説明。
[順序を変更したときにリブートする（Reboot on Order Change）] チェックボックス	このチェックボックスをオンにすると、ブートの順序を変更した後で、このブート ポリシーを使用するすべてのサーバがリブートされます。 オンにすると、CD-ROM またはフロッピーがブート順序の最後のデバイスである場合、デバイスの取り外しまたは装着をしても、ブート順には直接効力がないため、サーバはリブートされません。
[vNIC名またはvHBA名の適用（Enforce vNIC/vHBA Name）] チェックボックス	このチェックボックスをオンにすると、ブート順序表に記載されている 1 つ以上の vNIC、vHBA、iSCSI vNIC が、サービス プロファイルのサーバ設定と一致した場合に、設定エラーが表示されます。 オフにした場合、ポリシーはサービス プロファイル内のサーバ設定から vNIC、vHBA、または iSCSI vNIC（ブート オプションに適切なもの）を使用します。ブート ポリシーで指定されている vNIC、vHBA、iSCSI vNIC が、サービス プロファイルのサーバ設定と一致するかどうかについてはレポートされません。

名前	説明
[ブート モード（Boot Mode）] ドロップダウン リスト	このブート ポリシーを使用するサーバのブート モード。次のいずれかを設定できます。 • [レガシー（Legacy）] • [UEFI] このオプションでは、下位レベルのブート デバイスを指定し、セキュア ブート オプションを有効にできます。
[ブート セキュリティ（Boot Security）] チェックボックス	このブート ポリシーを使用するサーバのセキュア ブート オプションを有効にします。 このオプションは、[UEFI] がブート モードとして選択されている場合にのみ表示されます。

ステップ 8 [ローカル デバイスの追加（Add Local Device）] 領域で、[ローカル ディスクの追加（Add Local Disk）] チェックボックスをオンにします。
ローカル LUN、SD カード、CD ROM、内部および外部 USB デバイスのローカル ブート デバイスとしての追加などの、追加のセカンダリ オプションがあります。[ローカルディスクの追加（Add Local Disk）] チェックボックスをオンにすると、これらのセカンダリ デバイスはすべて選択できなくなります。これらのローカルデバイスのいずれかを選択すると、ローカルディスクの追加の上位オプションを選択できなくなります。

ステップ 9 [送信（Submit）] をクリックします。

仮想メディア ブート

サーバがアクセスできる仮想メディア デバイスから 1 つ以上のサーバをブートするよう、ブート ポリシーを設定することができます。仮想メディア デバイスは、物理 CD/DVD ディスク（読み取り専用）またはフロッピー ディスク（読み取り書き込み）のサーバへの挿入を疑似的に実行します。このタイプのサーバ ブートは、オペレーティング システムをサーバに手動でインストールする場合に使用するのが一般的です。

仮想メディア ブート ポリシーの作成

ブート ポリシーには、複数のタイプのブート デバイスを追加できます。たとえば、ローカル ディスク ブートをセカンダリ ブート デバイスとして追加できます。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 ポリシーを作成する組織をクリックして [詳細の表示（View Details）] をクリックします。

ステップ 5 [ブート ポリシー（Boot Policies）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [ブート ポリシーの追加（Add Boot Policy）] 画面で、次のフィールドに入力します。

名前	説明
[名前（Name）] フィールド	ポリシーの一意の名前。
[説明（Description）] フィールド	ポリシーの説明。
[順序を変更したときにリブートする（Reboot on Order Change）] チェックボックス	このチェックボックスをオンにすると、ブートの順序を変更した後で、このブートポリシーを使用するすべてのサーバがリブートされます。 このチェックボックスをオンにすると、CD-ROMまたはフロッピーがブート順序の最後のデバイスである場合、デバイスの取り外しまたは装着をしても、ブート順には直接効力がないため、サーバはリブートされません。
[vNIC名またはvHBA名の適用（Enforce vNIC/vHBA Name）] チェックボックス	このチェックボックスをオンにすると、ブート順序表に記載されている 1 つ以上の vNIC、vHBA、iSCSI vNIC が、サービス プロファイルのサーバ設定と一致した場合に、設定エラーが表示されます。 オフにした場合、ポリシーはサービスプロファイル内のサーバ設定からvNIC、vHBA、またはiSCSI vNIC（ブートオプションに適切なもの）を使用します。ブートポリシーで指定されている vNIC、vHBA、iSCSI vNIC が、サービス プロファイルのサーバ設定と一致するかどうかについてはレポートされません。

名前	説明
[ブート モード（Boot Mode）] ドロップダウン リスト	このブート ポリシーを使用するサーバのブート モード。次のいずれかを設定できます。 • [レガシー（Legacy）] • [UEFI] このオプションでは、下位レベルのブート デバイスを指定し、セキュア ブート オプションを有効にできます。
[ブート セキュリティ（Boot Security）] チェックボックス	このブート ポリシーを使用するサーバのセキュア ブート オプションを有効にします。 このオプションは、[UEFI] がブート モードとして選択されている場合にのみ表示されます。

ステップ 8 [ブート デバイスの追加（Add Boot Device）] 領域で、次のいずれかまたは両方のオプションをオンにして、ブート ポリシーに追加する vMedia デバイスを選択します。

- [CIMC マウント CD/DVD の追加（Add CIMC Mounted CD/DVD）]
- [CIMC マウント HDD の追加（Add CIMC Mounted HDD）]

ステップ 9 [送信（Submit）] をクリックします。

VMedia ポリシーと vMount の作成

vMedia を使用すると、外部イメージ ファイルをサーバの CIMC に動的にマッピングできます。vMedia ファイルが CDD としてマップされている場合、イメージ ファイルは CD-ROM イメージとして表示されます。vMedia は、サーバがブートを試みるブート ポリシーでデバイスとして参照できます。

vMedia ポリシーはサービス プロファイル（SP）にバインドされます。特定の SP はアクティブな vMedia ポリシーを 1 つだけ持てます。ただし、このポリシーには、1 つ以上の vMedia マウントを含めることができます。

（注） サービス プロファイルの vMedia ポリシーを変更しても、サービス プロファイルの再構成、再起動、またはサービスの中断は発生しません。

はじめる前に

Cisco UCS Manager、BIOS、およびCIMCの最小必要バージョンがあることを確認してください。『Cisco UCS Director Compatibility Matrix』を参照してください。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 更新する組織を選択し、[詳細の表示（View Details）] をクリックします。

ステップ 5 [vMedia ポリシー（vMedia Policy）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [vMedia ポリシーの追加（Add vMedia Policy）] 画面に、ポリシーの名前と説明を入力します。

ステップ 8 [マウント失敗時の再試行（Retry on Mount Failure）] ドロップダウンリストから、次のいずれかを選択して再試行モードを指定します。

- [はい（Yes）]：このオプションを選択すると、操作が成功するか、またはこのオプションが無効にされるまで、リモート サーバは vMedia のマウントを試行し続けます。
- [いいえ（No）]：このオプションを選択すると、マウントエラーが発生した場合、リモート サーバは vMedia を再度マウントしようとしません。

ステップ 9 [vMedia マウント ポイント（vMedia Mount Points）] を展開し、[追加（Add）] をクリックして、次の手順で新しい vMedia マウントを作成します。

a) [追加（Add）] をクリックします。

b) [vMedia マウント ポイントへのエントリの追加（Add Entry to vMedia Mount Points）] 画面で、次の必須フィールドに値を入力します。

- [デバイス タイプ（Device Type）]：[HDD] または [CDD] を選択します。各 vMedia ポリシーに対し、各デバイス タイプに 1 つずつ、最大 2 つの vMedia マウントを作成できます。
- [マウント名（Mount Name）]：vMedia マウントの一意の名前を入力します。
- [説明（Description）]：vMedia マウントの説明を入力します。入力できるのは最大 510 文字です。
- [プロトコル（Protocol）]：マウントされたリモート サーバとの通信に使用する、ネットワーク アクセスプロトコルを選択します。サポートされるプロトコルは、HTTPS、HTTP、CIFS、またはNFS です。タイプを選択した後、そのプロトコル タイプの追加パラメータを入力します。
  - プロトコルとして [HTTPS] を選択した場合は、リモート サーバにログインするための [ユーザ名（User Name）] と [パスワード（Password）] を入力します。

- プロトコルとして [HTTP] を選択した場合は、リモート サーバにログインするための [ユーザ名（User Name）] と [パスワード（Password）] を入力します。
- [CIFS] プロトコルを選択した場合は、マウントされたリモート サーバと通信するときに使用する認証プロトコルを選択します。認証プロトコルを選択しないと、[デフォルト（Default）] に設定されます。

  （オプション）：リモート サーバにログインするための [ユーザ名（User Name）] と [パスワード（Password）] を入力します。
- [NFS] プロトコルを選択した場合、追加のパラメータは必要ありません。

- [リモート サーバのホスト名/IP アドレス（Remote Server Host Name/IP Address）]：バックアップ ファイルを格納する場所のホスト名または IP アドレスを入力します。これは、サーバ、ストレージ アレイ、ローカル ドライブ、またはファブリック インターコネクトがネットワーク経由でアクセス可能な任意の読み取り/書き込みメディアなどがあります。

  （注） ホスト名を使用する場合は、DNS サーバを使用するように Cisco UCS ドメインを設定します。DNS 名は、インバンド ネットワークがそのサーバに設定されている場合に使用できます。
- [絶対リモート パス（Absolute Remote Path）]：リモート vMedia ファイルへのフル パスを入力します。

  （注） 選択したプロトコルが CIFS の場合は、パスにスラッシュを使用します。
- [サービス プロファイル名からファイル名を生成（Generate File Name from Service Profile Name）]：次のいずれかのオプションを選択します。
  - [なし（None）]：このオプションを選択する場合は、vMedia ポリシーで使用する必要があるリモート ファイル名を入力します。
  - [サービス プロファイル名（Service-Profile-Name）]：このオプションを選択すると、サービス プロファイル名がイメージ名として使用されます。

c) [送信（Submit）] をクリックします。

ステップ 10 [送信（Submit）] をクリックします。

iSCSI ブート

iSCSI ブートは、仮想インターフェイス カード（VIC アダプタ）を用いてサーバを有効にし、ネットワーク経由で離れた場所にある iSCSI ターゲット マシンからリモートで OS をブートします。Cisco UCS Director は、次のストレージによる iSCSI ブートをサポートしています。

- EMC VNX
- NetApp ONTAP

- NetApp Data Fabric Manager（DFM）
- NetApp C-Mode

Cisco UCS Director で iSCSI ブートを設定する場合は、まずの iSCSI ブートを設定し、次にの iSCSI ブート ワークフローを設定します。Cisco UCS DirectorCisco UCS

Cisco UCS 内の iSCSI ブートの詳細（実装ガイドラインなど）については、『Cisco UCS Manager configuration guides』を参照してください。

iSCSI ブートの前提条件

iSCSI ブートを設定するには、次の前提条件を満たしていることが必要です。

- ファームウェアを含む Cisco UCS ドメインが Cisco UCS リリース 2.0（1m）以降になっていること。
- Cisco UCS サーバに、次のようなサポートされている VIC アダプタが搭載されていること。
  - Cisco UCS M81KR 仮想インターフェイス カード
  - Cisco UCS VIC-1240 仮想インターフェイス カード
  - Cisco UCS VIC-1280 仮想インターフェイス カード
- ストレージ アレイで iSCSI ブートのライセンスを取得していること。
- アレイ側の LUN マスクおよびネットワーク インターフェイスが、iSCSI トラフィックで使用する VLAN にアクセスできるように適切に設定されていること。
- 適切な集約およびボリュームがストレージ アレイで作成されていること。
- ファブリック インターコネクトからのアップリンク ポートも iSCSI トラフィックの VLAN にアクセスできること。
- サーバのオペレーティング システム（OS）が、iSCSI ブート ファームウェア テーブル（iBFT）と互換性があること。

iSCSI ブートの設定

（注） この手順は、iSCSI ブート設定に必要な手順の概要です。次のすべてのステップを完了する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	iSCSI トラフィックの転送に必要な VLAN を作成します。	VLAN の作成を参照してください。
ステップ 2	該当する組織内のサーバに対し、1 つ以上の MAC プールを作成します。	MAC プールの作成を参照してください。
ステップ 3	該当する組織内の 1 つ以上の vNIC テンプレートを作成します。	vNIC テンプレートの作成を参照してください。
ステップ 4	ファブリック A とファブリック B の vNIC を作成します。	vNIC の作成を参照してください。
ステップ 5	これらの vNIC を含むネットワーク ポリシーを作成します。	ネットワーク ポリシーの作成を参照してください。
ステップ 6	ストレージ ポリシーを作成します。	ストレージ ポリシーの作成を参照してください。
ステップ 7	該当する組織内の 1 つ以上の IQN プールを作成します。	IQN プールの作成, （28 ページ）を参照してください。
ステップ 8	iSCSI IP プールの 1 つ以上の IP アドレス ブロックを作成します。	iSCSI IP プールへのアドレス ブロックの追加, （30 ページ）を参照してください。
ステップ 9	イニシエータとターゲット iSCSI認証プロファイルを作成します。	iSCSI 認証プロファイルの作成, （31 ページ）を参照してください。
ステップ 10	1 つ以上の iSCSI アダプタ ポリシーを作成します。	iSCSI アダプタ ポリシーの作成, （32 ページ）を参照してください。
ステップ 11	iSCSI ブート ワークフローを作成し、そのワークフローに必要なタスクを追加します。	次の例は、NetApp ONTAP ストレージの iSCSI ブート ワークフローを作成するワークフローを示したものです。 **1** 例：iSCSI ブート ワークフローの作成, （33 ページ） **2** タスクの追加：サービス プロファイルの作成, （35 ページ） **3** タスクの追加：サービス プロファイルへの vNIC の追加, （38 ページ）

	コマンドまたはアクション	目的
		4 タスクの追加：サービス プロファイルへの iSCSI vNIC の追加，（40 ページ）
		5 タスクの追加：サービス プロファイル iSCSI ブート ポリシーの作成，（42 ページ）
		6 タスクの追加：サービス プロファイルの関連付け，（44 ページ）
		7 タスクの追加：フレキシブル ボリュームの作成，（46 ページ）
		8 タスクの追加：LUN の作成，（48 ページ）
		9 タスクの追加：イニシエータ グループの作成，（49 ページ）
		10 タスクの追加：イニシエータ グループへのイニシエータの追加，（51 ページ）
		11 タスクの追加：イニシエータ グループへの LUN のマッピング，（52 ページ）
		12 タスクの追加：PXE ブートの設定，（54 ページ）
		13 タスクの追加：UCS サーバの電源をオンにする，（56 ページ）
		14 タスクの追加：PXE ブートのモニタリング，（57 ページ）
		15 タスクの追加：UCS サーバの電源をオフにする，（58 ページ）
		16 タスクの追加：iSCSI からブートするためのサービス プロファイル ブート ポリシーの変更，（59 ページ）
		17 2 つ目の [UCS サーバの電源をオンにする（Power On UCS Server）] タスクを追加します。

IQN プールの作成

IQN プールは、iSCSI vNIC が Cisco UCS ドメインでイニシエータ ID として使用する iSCSI 修飾名（IQN）の集合です。IQN プール メンバは、プレフィックス:サフィックス:数字 の形式になります。ここで、プレフィックス、サフィックス、および数字のブロック（範囲）を指定することが

できます。IQN プールは複数の IQN ブロックを含むことができます。それらは、数字の範囲とサフィックスは異なりますが、同じプレフィックスを共有します。

（注） 通常、最大 IQN サイズ（プレフィックス + サフィックス + 追加文字）は 223 文字です。Cisco UCS NIC M51KR-B アダプタを使用する場合、IQN サイズを 128 文字に制限します。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 プールを作成する組織をクリックして [詳細の表示（View Details）] をクリックします。

ステップ 5 [IQN プール（IQN Pools）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [IQN プールの作成（Create IQN Pool）] 画面で、名前と説明を定義する次のフィールドに入力します。

名前	説明
[名前（Name）] フィールド	iSCSI 修飾名（IQN）プールの一意の名前。
[説明（Description）] フィールド	プールのユーザ定義による説明。
[プレフィックス（Prefix）] フィールド	このプール用に作成された任意の IQN ブロックのプレフィックス。

ステップ 8 [次へ（Next）] をクリックします。

ステップ 9 [IQN ブロックの追加（Add IQN Blocks）] 画面で、次の手順を実行します。

a) [追加（Add）] をクリックします。

b) [IQN プール ブロックへのエントリの追加（Add Entry to IQN Pool Blocks）] ページで、次のフィールドに値を入力します。

名前	説明
[サフィックス（Suffix）] フィールド	この IQN のブロックのサフィックス。
[開始（From）] フィールド	ブロック内の最初のサフィックス番号。
[サイズ（Size）] フィールド	ブロック内のサフィックスの数。

c）[送信（Submit）] をクリックします。

必要なすべての IQN プール ブロックを追加するまで、この手順を繰り返します。

ステップ 10 [送信（Submit）] をクリックします。

iSCSI IP プールへのアドレス ブロックの追加

iSCSI IP プールは、iSCSI ブート用に確保されている IP アドレス グループです。この IP プールに、サーバまたはサービス プロファイルのスタティック IP アドレスとして割り当てられている IP アドレスが含まれていないことが必要です。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [iSCSI IP プール（iSCSI IP Pool）] をクリックします。

ステップ 4 [追加（Add）] をクリックします。

ステップ 5 [IP アドレスのブロックの作成（Create Block of IP Addresses）] 画面で、次のフィールドに値を入力します。

名前	説明
[開始（From）] フィールド	ブロック内の最初の IP アドレス。
[サイズ（Size）] フィールド	プール内の IP アドレスの数。
[サブネット マスク（Subnet Mask）] フィールド	ブロック内の IP アドレスに関連付けられたサブネット マスク。
[デフォルト ゲートウェイ（Default Gateway）] フィールド	ブロック内の IP アドレスに関連付けられたデフォルト ゲートウェイ。
[プライマリ DNS（Primary DNS）] フィールド	この IP アドレスのブロックがアクセスするプライマリ DNS サーバです。
[セカンダリ DNS（Secondary DNS）] フィールド	この IP アドレスのブロックがアクセスするセカンダリ DNS サーバです。

ステップ 6 [送信（Submit）] をクリックします。

iSCSI 認証プロファイルの作成

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 ポリシーを作成する組織をクリックして [詳細の表示（View Details）] をクリックします。

ステップ 5 [iSCSI 認証プロファイル（iSCSI Auth Profiles）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [iSCSI 認証プロファイル（iSCSI Authentication Profile）] 画面で、次のフィールドに値を入力します。

名前	説明
[名前（Name）] フィールド	iSCSI認証プロファイルの一意の名前。
[ユーザID（User ID）] フィールド	このプロファイルに関連付けられるユーザ ID。
[パスワード（Password）] フィールド	このプロファイルに関連付けられるパスワード。
[パスワードの確認（Confirm Password）] フィールド	確認のためのパスワードの再入力。

ステップ 8 [送信（Submit）] をクリックします。

iSCSI アダプタ ポリシーの作成

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 ポリシーを作成する組織をクリックして [詳細の表示（View Details）] をクリックします。

ステップ 5 [iSCSI アダプタ ポリシー（iSCSI Adapter Policy）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [iSCSI アダプタ ポリシー（iSCSI Adapter Policy）] 画面で、次のフィールドに値を入力します。

名前	説明
[名前（Name）] フィールド	ポリシーの一意の名前。
[接続タイムアウト（Connection Timeout）] フィールド	Cisco UCS が、初期サインインに失敗し、iSCSI アダプタが使用できないと判断するまでに待機する秒数。 0 ～ 255 の整数を入力します。0 を入力すると、Cisco UCS はアダプタ ファームウェアに設定された値（デフォルト：15 秒）を使用します。
[LUN再試行回数値の入力（LUN Busy Retry Count）] フィールド	iSCSI LUN 検出中にエラーが発生した場合に接続を再試行する回数。 0 ～ 60 の整数を入力します。0 を入力すると、Cisco UCS はアダプタ ファームウェアに設定された値（デフォルト：15 秒）を使用します。
[DHCPタイムアウト（DHCP Timeout）] フィールド	イニシエータが DHCP サーバが使用できないと判断するまでに待機する秒数。 60 ～ 300 の整数を入力します（デフォルトは 60 秒です）。
[TCPタイムスタンプの有効化（Enable TCP Timestamp）] チェックボックス	TCP タイムスタンプを使用する場合はこのチェックボックスをオンにします。この設定を使用すると、転送されるパケットにパケット送信時のタイムスタンプが付けられるので、必要なときにパケットのラウンドトリップ時間を計算することができます。 （注） このオプションは、Cisco UCS NIC M51KR-B アダプタを搭載したサーバにのみ適用されます。

名前	説明
[HBAモード（HBA Mode）] チェックボックス	HBA モード（TCP オフロードとも呼ばれます）を有効にする場合は、このチェックボックスをオンにします。 （注） このオプションは、Cisco UCS NIC M51KR-B アダプタを搭載し、Windows オペレーティング システムを実行しているサーバでのみ有効にする必要があります。
[ターゲットへのブート（Boot to Target）] チェックボックス	iSCSI ターゲットからブートする場合は、このチェックボックスをオンにします。 （注） このオプションは、Cisco UCS NIC M51KR-B アダプタを搭載したサーバにのみ適用されます。このオプションは、サーバにオペレーティング システムをインストールするまで無効にしておく必要があります。

ステップ 8 [送信（Submit）] をクリックします。

例：iSCSI ブート ワークフローの作成

この例では、NetApp ONTAP の iSCSI ブート ワークフローの作成方法を示します。Cisco UCS コンポーネントを設定する手順はストレージのすべてのタイプで同じです。

手順

ステップ 1 [オーケストレーション（Orchestration）] を選択します。

ステップ 2 [オーケストレーション（Orchestration）] ページで、[ワークフロー（Workflows）] をクリックします。

ステップ 3 [ワークフローの追加（Add Workflow）] をクリックします。

ステップ 4 [ワークフローの追加（Add Workflow）] 画面で、ワークフローの詳細を入力します。

名前	説明
[名前（Name）]フィールド	ワークフローの一意の名前。この名前によってワークフローの目的を説明することを推奨します。
[説明（Description）]フィールド	ワークフローの説明。

名前	説明
[ワークフローコンテキスト（Workflow Context）] ドロップダウン リスト	ワークフローを使用するコンテキストを選択します。次のいずれかになります。 • [任意（Any）]：任意のコンテキストでワークフローを使用できます。 • [選択済みのVM（Selected VM）]：ワークフローは VM が選択された場合に限り実行できます。
[複合タスクとして保存（Save as Compound Task）] チェックボックス	チェックマークをオンにすると、ワークフローを複合タスクとして定義します。
[新しいフォルダに配置（Place in New Folder）] チェックボックス	ワークフローを保存するフォルダ。このチェックボックスのチェックマークをオンにする場合は、フォルダ名を [フォルダ名（Folder Name）] フィールドに入力します。
[フォルダの選択（Select Folder）] ドロップダウン リスト	ワークフローを保存するフォルダを選択します。このドロップダウン リストは、[新しいフォルダに配置（Place in New Folder）] チェックボックスのチェックマークをオフにした場合のみ表示されます。

ステップ 5 [次へ（Next）] をクリックします。

ステップ 6 [ユーザ入力の追加（Add User Inputs）] ページで、次の手順を実行します。

a) [追加（Add）] をクリックします。

b) [ユーザ入力の追加（Add User Inputs）] 画面で、次のフィールドに値を入力し、[送信（Submit）] をクリックします。
必要なユーザ入力を用いてワークフローを設定する場合は、ワークフロー実行時の特定の値をプロンプト表示するワークフロー タスクを設定することができます。

名前	説明
[入力ラベル（Input Label）] フィールド	入力に割り当てられたラベル。
[入力の説明（Input Description）] フィールド	入力の説明。
[入力タイプ（Input Type）] フィールド	入力カテゴリのタイプ。

名前	説明
[管理者の入力値（Admin Input）] フィールド	入力タイプに基づく管理者からの入力。ワークフローを実行するエンドユーザが入力を提供する必要はありません。管理者はエンド ユーザに対して、特定のタイプの入力を禁止することもできます。
[管理入力リスト（Admin Input List）] フィールド	現在の管理者の入力リスト。入力順序を再配置することができます。
[管理入力フィルタ（Admin Input Filter）] フィールド	管理者の入力フィルタ値。カスタム入力をフィルタに基づいて（静的または動的に）定義するための値です。たとえば、集約、ボリューム、および POD にフィルタを適用できます

ユーザ追加入力を追加する場合は、この手順を繰り返します。

ステップ 7 [送信（Submit）] をクリックします。
ワークフローを新規フォルダに作成した場合は、[更新（Refresh）] をクリックしてフォルダ リストのフォルダを表示する必要がある場合があります。

次の作業

タスクを空のワークフローに追加します。

タスクの追加：サービス プロファイルの作成

この手順は、例：iSCSI ブート ワークフローの作成, （33 ページ） に基づいてワークフローを作成済みで、オーケストレーション内に [ワークフロー（Workflow）] タブが表示されていることを前提としています。

手順

ステップ 1 [オーケストレーション（Orchestration）] を選択します。

ステップ 2 [オーケストレーション（Orchestration）] ページで、[ワークフロー（Workflows）] をクリックします。

ステップ 3 タスクを追加する iSCSI ワークフローの行をクリックします。

ステップ 4 [その他のアクション（More Actions）] ドロップダウン リストから [ワークフロー デザイナ（Workflow Designer）] を選択します。

ステップ 5 ワークフロー デザイナの [使用可能なタスク（Available Tasks）] 画面で [物理コンピューティング タスク（Physical Compute Tasks）] > [Cisco UCS タスク（Cisco UCS Tasks）] を展開します。

ステップ 6 [UCSサービスプロファイルの作成（Create UCS Service Profile）] タスクをクリックし、選択したタスクをワークフロー デザイナ ウィンドウにドラッグ アンド ドロップします。

ステップ 7 [タスク情報（Task Information）] 画面で、次の操作を実行します。

a) タスクを識別するタスク名とコメントを入力します。

b) エラーが発生した場合に、Cisco UCS Director でワークフローを自動的に再試行できるようにするには、次の手順を実行します。

- [再試行の実行（Retry Execution）] チェックボックスをオンにします。
- [再試行回数（Retry Count）] ドロップダウン リストから、再試行する回数を選択します。
- [再試行の頻度（Retry Frequency）] フィールドに、再試行間の秒数を示すコンマ区切りの値リストを入力します。

c) タスクの詳細を確認します。

d) [次へ（Next）] をクリックします。

ステップ 8 [ユーザ マッピング入力（User Mapping Inputs）] 画面で、次の手順を実行します。

a) ワークフロー実行時にサービスプロファイルの設定属性の一部を入力するプロンプトを表示したい場合は、次のチェックボックスの 1 つまたは複数をオンにして、ユーザ入力を選択します。

（注） ユーザ入力をマッピングするには、ワークフローにユーザ入力と適切な許可を追加する必要があります。

- [サービスプロファイル名（Service Profile Name）]
- [説明（Description）]
- [組織（Organization）]
- [ストレージポリシー（Storage Policy）]
- [ネットワークポリシー（Network Policy）]
- [PXEブートポリシー（PXE Boot Policy）]
- [サーバブートポリシー（Server Boot Policy）]

- [IPアドレス（IP Address）]
- [サブネット マスク（Subnet Mask）]
- [デフォルトゲートウェイ（Default Gateway）]
- [サーバの電源状態（Server Power State）]

b) [次へ（Next）] をクリックします。

ステップ 9 [タスク入力（Task Inputs）] 画面で、次の操作を実行します。

a) ユーザ入力のプロンプトの表示を選択しなかったこれらの設定属性については、次の手順を実行します。

- [サービスプロファイル名（Service Profile Name）] : 必須項目です。サービス プロファイルの一意の名前を入力します。
- [説明（Description）] : 任意項目です。サービス プロファイルの説明を入力します。
- [組織（Organization）] : 必須項目です。ワークフローを実行し、サービス プロファイルを作成する組織を選択します。この項目では、ワークフローの Cisco UCS Manager アカウントを選択できます。
- [UUID の割り当て（UUID Assignment）] : 必須項目です。このポリシーを選択すると、サーバの UUID を指定できます。
- [ストレージポリシー（Storage Policy）] : 必須項目です。iSCSI ブートに作成するストレージ ポリシーを指定します。
- [ネットワークポリシー（Network Policy）] : 必須項目です。ネットワーク ポリシーを指定します。
- [配置ポリシー（Placement Policy）] : 任意項目です。このポリシーを選択すると、サーバの vNIC、vHBA、vCon の配置を指定できます。
- [PXEブートポリシー（PXE Boot Policy）] : 任意項目です。 このポリシーを選択すると、サーバで PXE ブートを実行できます。このポリシーのセカンダリ ブートは、ローカル ディスクまたは SAN ブートにする必要があります。このポリシーを選択しない場合は、ブート順序の決定時にサーバ ブート ポリシーが使用されます。
- [サーバブートポリシー（Server Boot Policy）] : 必須項目です。このポリシーを選択すると、サーバのブート順序を決定できます。
- [BIOSポリシー（BIOS Policy）] : 任意項目です。このポリシーを選択すると、サーバの BIOS のデフォルト設定を変更できます。
- [IPMI アクセス プロファイル（IPMI Access Profile）] : 任意項目です。このポリシーを選択すると、IPMI 経由でサーバにアクセスできます。
- [SOL 設定プロファイル（SOL Configuration Profile）] : 任意項目です。このポリシーを選択すると、Serial over LAN 経由でサーバにアクセスできます。

- [しきい値ポリシー（Threshold Policy）]：任意項目です。このポリシーを選択すると、サーバのしきい値を指定できます。
- [スクラビング ポリシー（Scrub Policy）]：任意項目です。このポリシーを選択すると、検出時や関連付け解除時のサーバのローカル データやBIOS 設定に対する動作を指定できます。
- [ホスト ファームウェア ポリシー（Host Firmware Policy）]：任意項目です。このポリシーを選択すると、ホスト ファームウェア パッケージを使用して、サーバ ファームウェアをアップグレードできます。
- [メンテナンス ポリシー（Maintenance Policy）]：任意項目です。このポリシーを選択すると、このサービス プロファイルにサーバのリブートが必要な変更が加えられた際の動作を指定できます。
- [電源制御ポリシー（Power Control Policy）]：任意項目です。このポリシーを選択すると、サービス プロファイルをブレード サーバと関連付けて、サーバの初期電源割り当てを指定できます。
- [サーバの電源状態（Server Power State）]：必須項目です。サービス プロファイルと関連付けられた際にサーバに適用される電源消費状態を設定します。

b) [送信（Submit）] をクリックします。

タスクの追加：サービス プロファイルへの vNIC の追加

このタスクは、iSCSI vNIC のオーバーレイ vNIC として機能するサービス プロファイルに、3 つ目の vNIC を追加します。

手順

ステップ 1 [オーケストレーション（Orchestration）] を選択します。

ステップ 2 [オーケストレーション（Orchestration）] ページで、[ワークフロー（Workflows）] をクリックします。

ステップ 3 タスクを追加する iSCSI ワークフローの行をクリックします。

ステップ 4 [その他のアクション（More Actions）] ドロップダウン リストから [ワークフロー デザイナ（Workflow Designer）] を選択します。

ステップ 5 ワークフロー デザイナの [使用可能なタスク（Available Tasks）] 画面で [物理コンピューティング タスク（Physical Compute Tasks）] > [Cisco UCS タスク（Cisco UCS Tasks）] を展開します。

ステップ 6 [サービス プロファイルへの vNIC の追加（Add vNIC to Service Profile）] タスクをクリックし、選択したタスクをワークフロー デザイナ ウィンドウにドラッグ アンド ドロップします。

ステップ 7 [タスク情報（Task Information）] 画面で、次の操作を実行します。

a) タスクを識別するタスク名とコメントを入力します。

b) エラーが発生した場合に、Cisco UCS Director でワークフローを自動的に再試行できるようにするには、次の手順を実行します。

- [再試行の実行（Retry Execution）] チェックボックスをオンにします。
- [再試行回数（Retry Count）] ドロップダウン リストから、再試行する回数を選択します。
- [再試行の頻度（Retry Frequency）] フィールドに、再試行間の秒数を示すコンマ区切りの値リストを入力します。

c) タスクの詳細を確認します。

d) [次へ（Next）] をクリックします。

ステップ 8 [ユーザ マッピング入力（User Mapping Inputs）] 画面で、次の手順を実行します。

a) ワークフロー実行時に vNIC の設定属性の一部を入力するプロンプトを表示したい場合は、次のチェックボックスの 1 つまたは複数をオンにして、ユーザ入力を選択します。

（注） ユーザ入力をマッピングするには、ワークフローにユーザ入力と適切な許可を追加する必要があります。

- [サービスプロファイル（Service Profile）] : vNIC を追加する既存のサービス プロファイルを選択します。
- [vNIC名（vNIC Name）] : 既存の vNIC をサービス プロファイルに追加します。

b) [次へ（Next）] をクリックします。

ステップ 9 [タスク入力（Task Inputs）] 画面で、次の操作を実行します。

a) ユーザ入力のプロンプトの表示を選択しなかったこれらの設定属性については、次の手順を実行します。
新しい vNIC を作成してサービス プロファイルに追加する場合は、このオプションを使用します。

- [サービスプロファイル名（Service Profile Name）] : 必須項目です。iSCSI ブートを設定する既存のサービス プロファイルを選択します。
- [vNIC名（vNIC Name）] : 必須項目です。
- [MACプール（MAC Pool）] : 必須項目です。
- [ファブリックID（Fabric ID）] : 必須項目です。
- [フェールオーバーの有効化（Enable Failover）] : 必須項目です。このチェックボックスをオンにします。
- [VLAN] : 必須項目です。iSCSI トラフィックの転送用に作成した VLAN を選択します。
- [ネイティブVLANとして設定（Set as Native VLAN）] : 任意項目です。
- [MTU] : 必須項目です。1500 から 9000 までの値を入力してください。
- [ピングループ（Pin Group）] : 任意項目です。
- [アダプタポリシー（Adapter Policy）] : 任意項目です。

- [QoSポリシー（QoS Policy）]：任意項目です。
- [ネットワーク制御ポリシー（Network Control Policy）]：任意項目です。
- [統計しきい値ポリシー（Stats Threshold Policy）]：任意項目です。

b) [送信（Submit）] をクリックします。

タスクの追加：サービス プロファイルへの iSCSI vNIC の追加

手順

ステップ 1 [オーケストレーション（Orchestration）] を選択します。

ステップ 2 [オーケストレーション（Orchestration）] ページで、[ワークフロー（Workflows）] をクリックします。

ステップ 3 タスクを追加する iSCSI ワークフローの行をクリックします。

ステップ 4 [その他のアクション（More Actions）] ドロップダウン リストから [ワークフロー デザイナ（Workflow Designer）] を選択します。

ステップ 5 ワークフロー デザイナの [使用可能なタスク（Available Tasks）] 画面で [物理コンピューティング タスク（Physical Compute Tasks）] > [Cisco UCS タスク（Cisco UCS Tasks）] を展開します。

ステップ 6 [サービス プロファイルへの iSCSI vNIC の追加（Add iSCSI vNIC to Service Profile）] タスクをクリックし、選択したタスクをワークフロー デザイナ ウィンドウにドラッグ アンド ドロップします。

ステップ 7 [タスク情報（Task Information）] 画面で、次の操作を実行します。

a) タスクを識別するタスク名とコメントを入力します。

b) エラーが発生した場合に、Cisco UCS Director でワークフローを自動的に再試行できるようにするには、次の手順を実行します。

- [再試行の実行（Retry Execution）] チェックボックスをオンにします。
- [再試行回数（Retry Count）] ドロップダウン リストから、再試行する回数を選択します。
- [再試行の頻度（Retry Frequency）] フィールドに、再試行間の秒数を示すコンマ区切りの値リストを入力します。

c) タスクの詳細を確認します。

d) [次へ（Next）] をクリックします。

ステップ 8 [ユーザ マッピング入力（User Mapping Inputs）] 画面で、次の手順を実行します。

a) ワークフロー実行時に vNIC の設定属性の一部を入力するプロンプトを表示したい場合は、次のチェックボックスの 1 つまたは複数をオンにして、ユーザ入力を選択します。

（注） ユーザ入力をマッピングするには、ワークフローにユーザ入力と適切な許可を追加する必要があります。

- [サービスプロファイル（Service Profile）]：vNIC を追加するサービス プロファイルのプロンプトです。
- [iSCI vNIC名（iSCI vNIC Name）]：既存の iSCSI vNIC をサービス プロファイルに追加します。
- [オーバーレイvNIC名（Overlay vNIC Name）]：既存のオーバーレイ vNIC を使用します。
- [VLAN]：既存の VLAN を使用します。

b) [次へ（Next）] をクリックします。

ステップ 9 [タスク入力（Task Inputs）] 画面で、次の操作を実行します。

a) ユーザ入力のプロンプトの表示を選択しなかったこれらの設定属性については、次の手順を実行します。

- [サービスプロファイル名（Service Profile Name）]：必須項目です。iSCSI ブートを設定する既存のサービス プロファイルを選択します。
- [iSCSI vNIC名（iSCSI vNIC Name）]：必須項目です。
- [オーバーレイvNIC（Overlay vNIC）]：必須項目です。サービス プロファイルに追加した 3 つ目の vNIC を選択します。
- [iSCSIアダプタポリシー（iSCSI Adapter Policy）]：任意項目です。
- [MACプール（MAC Pool）]：MAC プールを選択しないでください。
- [VLAN]：必須項目です。iSCSI トラフィックの転送用に作成した VLAN を選択します。

b) [送信（Submit）] をクリックします。

タスクの追加：サービス プロファイル iSCSI ブート ポリシーの作成

手順

ステップ 1 [オーケストレーション（Orchestration）] を選択します。

ステップ 2 [オーケストレーション（Orchestration）] ページで、[ワークフロー（Workflows）] をクリックします。

ステップ 3 タスクを追加する iSCSI ワークフローの行をクリックします。

ステップ 4 [その他のアクション（More Actions）] ドロップダウン リストから [ワークフロー デザイナ（Workflow Designer）] を選択します。

ステップ 5 ワークフロー デザイナの [使用可能なタスク（Available Tasks）] 画面で [物理コンピューティング タスク（Physical Compute Tasks）] > [Cisco UCS タスク（Cisco UCS Tasks）] を展開します。

ステップ 6 [サービスプロファイルiSCSIブートポリシーの作成（Create Service Profile iSCSI Boot Policy）] タスクをクリックし、選択したタスクをワークフローデザイナ ウィンドウにドラッグ アンド ドロップします。

ステップ 7 [タスク情報（Task Information）] 画面で、次の操作を実行します。

a) タスクを識別するタスク名とコメントを入力します。

b) エラーが発生した場合に、Cisco UCS Director でワークフローを自動的に再試行できるようにするには、次の手順を実行します。

- [再試行の実行（Retry Execution）] チェックボックスをオンにします。
- [再試行回数（Retry Count）] ドロップダウン リストから、再試行する回数を選択します。
- [再試行の頻度（Retry Frequency）] フィールドに、再試行間の秒数を示すコンマ区切りの値リストを入力します。

c) タスクの詳細を確認します。

d) [次へ（Next）] をクリックします。

ステップ 8 [ユーザ マッピング入力（User Mapping Inputs）] 画面で、次の手順を実行します。

a) ワークフロー実行時にポリシーの設定属性の一部を入力するプロンプトを表示したい場合は、次のチェックボックスの 1 つまたは複数をオンにして、ユーザ入力を選択します。

（注） ユーザ入力をマッピングするには、ワークフローにユーザ入力と適切な許可を追加する必要があります。

- [サービスプロファイル（Service Profile）] : 既存のサービス プロファイルを使用して、iSCSI ブート ポリシーを作成します。
- [プライマリ vNIC（Primary vNIC）] : 既存の vNIC を LAN ブートのプライマリ vNIC として追加します。
- [セカンダリ vNIC（Secondary vNIC）] : 既存の vNIC を LAN ブートのセカンダリ vNIC として追加します。

- [プライマリiSCSI vNIC（Primary iSCSI vNIC）]：既存の iSCSI vNIC をプライマリ iSCSI vNIC として追加します。
- [ファイラの選択（Select Filer）]：LUN が作成された既存のファイラまたは vFiler を選択できます。
- [iSCSIターゲット名（iSCSI Target Name）]：ファイラのターゲット ノード名を指定できます。
- [IPv4アドレス（IPv4 Address）]：ファイラの iSCSI 対応 VLAN IP アドレスを指定できます。

b) [次へ（Next）] をクリックします。

ステップ 9 [タスク入力（Task Inputs）] 画面で、次の操作を実行します。

a) ユーザ入力のプロンプトの表示を選択しなかったこれらの設定属性については、次の手順を実行します。

名前	説明
[サービスプロファイル（Service Profile）] ボタン	iSCSI ブートを設定する既存のサービス プロファイルを選択します。
[LANブートの追加（Add LAN Boot）] チェックボックス	チェックボックスをオンにすると、ポリシーにLANブートが追加されます。
[プライマリvNIC（Primary vNIC）] フィールド	LAN ブートに使用するプライマリ vNIC です。 このフィールドは、[LANブートの追加（Add LAN Boot）] チェックボックスをオンにした場合にのみ表示されます。
[セカンダリvNIC（Secondary vNIC）] フィールド	LAN ブートに使用するセカンダリ vNIC です。 このフィールドは、[LANブートの追加（Add LAN Boot）] チェックボックスをオンにした場合にのみ表示されます。
[ブートパラメータの設定（Set Boot Parameters）] チェックボックス	チェックボックスをオンにすると、iSCSI ブート パラメータが設定されます。 次のフィールドは、このチェックボックスをオンにした場合にのみ表示されます。
[iSCSIブートパラメータの設定（Set iSCSI Boot Parameters）] 領域	
[認証プロファイル（Authentication Profile）] ボタン	iSCSI 認証プロファイルを作成します。

名前	説明
[イニシエータ名の割り当て（Initiator Name Assignment）] ボタン	イニシエータが iSCSI vNIC に割り当てられる IQN プールを選択します。
[イニシエータのIPアドレスポリシー（Initiator IP Address Policy）] ドロップダウン リスト	iSCSI vNIC への IP アドレスの割り当て方法を選択します。デフォルトでは、IP アドレスは iSCSI IP プールから割り当てられます。
[iSCSI静的ターゲットの作成（Create iSCSI Static Target）] 領域	
[ファイラの選択（Select Filer）] ボタン	ターゲットに関連付けられている LUN が作成されるファイラ（NetApp ファイラや vFiler など）を選択します。
[iSCSIターゲット名（iSCSI Target Name）] ドロップダウン リスト	ファイラのターゲット ノードを選択します。
[ポート（Port）] フィールド	ストレージ アレイの接続に使用されるポート ID です。
[認証プロファイル（Authentication Profile）] ボタン	関連付けられている iSCSI 認証プロファイルを選択します。
[IPv4アドレス（IPv4 Address）] ドロップダウン リスト	ファイラの iSCSI 対応 VLAN IP アドレスを選択します。
[LUN ID] フィールド	iSCSI ターゲットの LUN 識別子です。

b) [送信（Submit）] をクリックします。

タスクの追加：サービス プロファイルの関連付け

この手順は、例：iSCSI ブート ワークフローの作成, （33 ページ） に基づいてワークフローを作成済みで、オーケストレーション内に [ワークフロー（Workflow）] タブが表示されていることを前提としています。

手順

ステップ 1 [オーケストレーション（Orchestration）] を選択します。

ステップ 2 [オーケストレーション（Orchestration）] ページで、[ワークフロー（Workflows）] をクリックします。

ステップ 3 タスクを追加する iSCSI ワークフローの行をクリックします。

ステップ 4 [その他のアクション（More Actions）] ドロップダウン リストから [ワークフロー デザイナ（Workflow Designer）] を選択します。

ステップ 5 ワークフロー デザイナの [使用可能なタスク（Available Tasks）] 画面で [物理コンピューティング タスク（Physical Compute Tasks）] > [Cisco UCS タスク（Cisco UCS Tasks）] を展開します。

ステップ 6 [UCSサービスプロファイルの関連付け（Associate UCS Service Profile）] タスクをクリックし、選択したタスクをワークフロー デザイナ ウィンドウにドラッグ アンド ドロップします。

ステップ 7 [タスク情報（Task Information）] 画面で、次の操作を実行します。

a) タスクを識別するタスク名とコメントを入力します。

b) エラーが発生した場合に、Cisco UCS Director でワークフローを自動的に再試行できるようにするには、次の手順を実行します。

- [再試行の実行（Retry Execution）] チェックボックスをオンにします。
- [再試行回数（Retry Count）] ドロップダウン リストから、再試行する回数を選択します。
- [再試行の頻度（Retry Frequency）] フィールドに、再試行間の秒数を示すコンマ区切りの値リストを入力します。

c) タスクの詳細を確認します。

d) [次へ（Next）] をクリックします。

ステップ 8 [タスクの追加（UCSサービスプロファイルの関連付け）（Add Task (Associate UCS Service Profile)）] ウィザードの [ユーザマッピング入力（User Mapping Inputs）] 画面で、次の手順を実行します。

a) ワークフロー実行時に設定属性の一部を入力するプロンプトを表示したい場合は、次のチェックボックスの 1 つまたは複数をオンにして、ユーザ入力を選択します。

（注） ユーザ入力をマッピングするには、ワークフローにユーザ入力と適切な許可を追加する必要があります。

- [サービスプロファイル（Service Profile）]：サーバと関連付けるサービス プロファイルを選択します。
- [サーバ（Server）]：サービス プロファイルと関連付けるサーバを選択します。
- [サーバプール（Server Pool）]：サービス プロファイルと関連付けるサーバのタイプが含まれるサーバ プールを選択します。

b) [次へ（Next）] をクリックします。

ステップ 9 [タスクの追加（UCSサービスプロファイルの関連付け）（Add Task (Associate UCS Service Profile)）] ウィザードの [タスク入力（Task Inputs）] 画面で、次の手順を実行します。

a) ユーザ入力のプロンプトの表示を選択しなかったこれらの設定属性については、次の手順を実行します。

- [サービスプロファイル（Service Profile）]：必須項目です。iSCSI ブートを設定する既存のサービス プロファイルを選択します。
- [サーバの選択範囲（Server Selection Scope）]：必須項目です。サーバの選択方法を選択します。
- [サーバ（Server）]：[サーバを含む（Include Servers）] の範囲を選択した場合は、必須項目です。サービス プロファイルと関連付けるサーバを選択します。
- [サーバプール（Server Pool）]：[サーバプールを含む（Include Server Pools）] の範囲を選択した場合は、必須項目です。サービス プロファイルと関連付けるサーバのタイプが含まれるサーバ プールを選択します。

b) [送信（Submit）] をクリックします。

タスクの追加：フレキシブル ボリュームの作成

ESXi のインストールには、12 GB 以上のボリュームを作成することをお勧めします。

手順

ステップ 1 [オーケストレーション（Orchestration）] を選択します。

ステップ 2 [オーケストレーション（Orchestration）] ページで、[ワークフロー（Workflows）] をクリックします。

ステップ 3 タスクを追加する iSCSI ワークフローの行をクリックします。

ステップ 4 [その他のアクション（More Actions）] ドロップダウン リストから [ワークフロー デザイナ（Workflow Designer）] を選択します。

ステップ 5 ワークフロー デザイナの [使用可能なタスク（Available Tasks）] 画面で、[物理ストレージ タスク（Physical Storage Tasks）] > [NetApp タスク（NetApp Tasks）] > [NetApp ONTAP タスク（NetApp ONTAP Tasks）] を展開します。

ステップ 6 [フレキシブルボリュームの作成（Create Flexible Volume）] タスクをクリックし、選択したタスクをワークフロー デザイナ ウィンドウにドラッグ アンド ドロップします。

ステップ 7 [タスクの追加（フレキシブルボリュームの作成）（Add Task (Create Flexible Volume)）] ウィザードの [タスク情報（Task Information）] 画面で、次の手順を実行します。

a) タスクを識別するタスク名とコメントを入力します。

b) エラーが発生した場合に、Cisco UCS Director でワークフローを自動的に再試行できるようにするには、次の手順を実行します。

- [再試行の実行（Retry Execution）] チェックボックスをオンにします。
- [再試行回数（Retry Count）] ドロップダウン リストから、再試行する回数を選択します。

- [再試行の頻度（Retry Frequency）] フィールドに、再試行間の秒数を示すコンマ区切りの値リストを入力します。

c) タスクの詳細を確認します。
d) [次へ（Next）] をクリックします。

ステップ 8 [タスクの追加（フレキシブルボリュームの作成）（Add Task (Create Flexible Volume)）] ウィザードの [ユーザマッピング入力（User Mapping Inputs）] 画面で、次の手順を実行します。

a) ワークフロー実行時にボリュームの設定属性の一部を入力するプロンプトを表示したい場合は、次のチェックボックスの 1 つまたは複数をオンにして、ユーザ入力を選択します。
（注） ユーザ入力をマッピングするには、ワークフローにユーザ入力と適切な許可を追加する必要があります。

- [集約名（Aggregate Name）] : ボリュームを作成する集約を選択します。
- [ボリューム名（Volume Name）] : ボリュームに名前を割り当てます。
- [ボリュームサイズ（Volume Size）] : ボリュームのサイズを整数で指定します。
- [ボリュームサイズユニット（Volume Size Units）] : サイズ単位（MB、GB、TB など）を選択します。
- [容量保証（Space Guarantee）] : 容量保証のタイプを指定します。
- [スナップショットサイズ（Snapshot Size）] : ボリューム スナップショットのパーセントを指定します。

b) [次へ（Next）] をクリックします。

ステップ 9 [タスクの追加（フレキシブルボリュームの作成）（Add Task (Create Flexible Volume)）] ウィザードの [タスク入力（Task Inputs）] 画面で、次の手順を実行します。

a) ユーザ入力のプロンプトの表示を選択しなかったこれらの設定属性については、次の手順を実行します。

- [集約名（Aggregate Name）] : ボリュームを作成する集約を選択します。
- [ボリューム名（Volume Name）] : ボリュームの一意の名前を入力します。
- [ボリュームサイズ（Volume Size）] : ボリュームのサイズを整数で入力します。以下を設定する必要があります。
- [ボリュームサイズユニット（Volume Size Units）] : サイズ単位を選択します。
- [容量保証（Space Guarantee）] : 容量保証のタイプを選択します。
- [スナップショットサイズ（Snapshot Size）] : ボリューム スナップショットのパーセントを入力します。
- [セキュリティスタイルNTFS（Security Style NTFS）] : このチェック ボックスはオンにしないでください。
- [NFSエクスポート（NFS Export）] : このチェック ボックスはオンにしないでください。

b) [送信（Submit）] をクリックします。

タスクの追加：LUN の作成

ESXi のインストールには、10 GB 以上の LUN を作成することをお勧めします。

手順

ステップ 1 [オーケストレーション（Orchestration）] を選択します。

ステップ 2 [オーケストレーション（Orchestration）] ページで、[ワークフロー（Workflows）] をクリックします。

ステップ 3 タスクを追加する iSCSI ワークフローの行をクリックします。

ステップ 4 [その他のアクション（More Actions）] ドロップダウン リストから [ワークフロー デザイナ（Workflow Designer）] を選択します。

ステップ 5 ワークフロー デザイナの [使用可能なタスク（Available Tasks）] 画面で、[物理ストレージ タスク（Physical Storage Tasks）] > [NetApp タスク（NetApp Tasks）] > [NetApp ONTAP タスク（NetApp ONTAP Tasks）] を展開します。

ステップ 6 [LUN の作成（Create LUN）] タスクをクリックし、選択したタスクをワークフローデザイナ ウィンドウにドラッグ アンド ドロップします。

ステップ 7 [タスク情報（Task Information）] 画面で、次の操作を実行します。

a) タスクを識別するタスク名とコメントを入力します。

b) エラーが発生した場合に、Cisco UCS Director でワークフローを自動的に再試行できるようにするには、次の手順を実行します。

- [再試行の実行（Retry Execution）] チェックボックスをオンにします。
- [再試行回数（Retry Count）] ドロップダウン リストから、再試行する回数を選択します。
- [再試行の頻度（Retry Frequency）] フィールドに、再試行間の秒数を示すコンマ区切りの値リストを入力します。

c) タスクの詳細を確認します。

d) [次へ（Next）] をクリックします。

ステップ 8 [ユーザ マッピング入力（User Mapping Inputs）] 画面で、次の手順を実行します。

a) ワークフロー実行時にボリュームの設定属性の一部を入力するプロンプトを表示したい場合は、次のチェックボックスの 1 つまたは複数をオンにして、ユーザ入力を選択します。

（注） ユーザ入力をマッピングするには、ワークフローにユーザ入力と適切な許可を追加する必要があります。

- [ボリューム名（Volume Name）]：LUN を作成するボリュームを指定します。
- [LUN名（LUN Name）]：作成する LUN の名前を指定します。

- [OSタイプ（OS Type）]：LUN の OS タイプを指定します。
- [LUNサイズ（LUN Size）]：LUN のサイズを整数で指定します。
- [LUNサイズ単位（LUN Size Units）]：サイズ単位（MB、GB、TB など）を指定します。

b) [次へ（Next）] をクリックします。

ステップ 9 [タスク入力（Task Inputs）] 画面で、次の操作を実行します。

a) ユーザ入力のプロンプトの表示を選択しなかったこれらの設定属性については、次の手順を実行します。

- [ボリューム名（Volume Name）]：LUN を作成するボリュームを選択します。
- [LUN名（LUN Name）]：作成する LUN の名前を入力します。
- [OSタイプ（OS Type）]：LUN の OS タイプを選択します。
- [LUNサイズ（LUN Size）]：LUN のサイズを整数で入力します。
- [LUNサイズ単位（LUN Size Units）]：サイズ単位（MB、GB、TB など）を選択します。
- [予約済み容量（Reserve Space）]：このチェックボックスをオンにすると、LUN の容量が予約されます。

b) [送信（Submit）] をクリックします。

タスクの追加：イニシエータ グループの作成

手順

ステップ 1 [オーケストレーション（Orchestration）] を選択します。

ステップ 2 [オーケストレーション（Orchestration）] ページで、[ワークフロー（Workflows）] をクリックします。

ステップ 3 タスクを追加する iSCSI ワークフローの行をクリックします。

ステップ 4 [その他のアクション（More Actions）] ドロップダウン リストから [ワークフロー デザイナ（Workflow Designer）] を選択します。

ステップ 5 ワークフロー デザイナの [使用可能なタスク（Available Tasks）] 画面で、[物理ストレージ タスク（Physical Storage Tasks）] > [NetApp タスク（NetApp Tasks）] > [NetApp ONTAP タスク（NetApp ONTAP Tasks）] を展開します。

ステップ 6 [イニシエータグループの作成（Create Initiator Group）] タスクをクリックし、選択したタスクをワークフロー デザイナ ウィンドウにドラッグ アンド ドロップします。

ステップ 7 [タスク情報（Task Information）] 画面で、次の操作を実行します。

a) タスクを識別するタスク名とコメントを入力します。

b) エラーが発生した場合に、Cisco UCS Director でワークフローを自動的に再試行できるようにするには、次の手順を実行します。

- [再試行の実行（Retry Execution）] チェックボックスをオンにします。
- [再試行回数（Retry Count）] ドロップダウン リストから、再試行する回数を選択します。
- [再試行の頻度（Retry Frequency）] フィールドに、再試行間の秒数を示すコンマ区切りの値リストを入力します。

c) タスクの詳細を確認します。

d) [次へ（Next）] をクリックします。

ステップ 8 [タスクの追加（イニシエータグループの作成）（Add Task (Create Initiator Group)）] ウィザードの [ユーザマッピング入力（User Mapping Inputs）] 画面で、次の手順を実行します。

a) ワークフロー実行時にボリュームの設定属性の一部を入力するプロンプトを表示したい場合は、次のチェックボックスの 1 つまたは複数をオンにして、ユーザ入力を選択します。

（注） ユーザ入力をマッピングするには、ワークフローにユーザ入力と適切な許可を追加する必要があります。

- [ファイラID名（Filer Identity Name）] : イニシエータ グループを作成するファイラを指定します。
- [イニシエータグループ名（Initiator Group Name）] : 作成するイニシエータ グループの名前を指定します。
- [グループタイプ（Group Type）] : イニシエータ グループのタイプの iSCSI を指定します。
- [OSタイプ（OS Type）] : グループ内のイニシエータの OS タイプを指定します。
- [ポートセット（Port Set）] : ポート セットを指定します。

b) [次へ（Next）] をクリックします。

ステップ 9 [タスクの追加（イニシエータグループの作成）（Add Task (Create Initiator Group)）] ウィザードの [タスク入力（Task Inputs）] 画面で、次の手順を実行します。

a) ユーザ入力のプロンプトの表示を選択しなかったこれらの設定属性については、次の手順を実行します。

- [ファイラID名（Filer Identity Name）] : イニシエータ グループを作成するファイラを選択します。
- [イニシエータグループ名（Initiator Group Name）] : 作成するイニシエータ グループの名前を入力します。
- [グループタイプ（Group Type）] : イニシエータ グループのタイプの iSCSI を選択します。
- [OSタイプ（OS Type）] : グループ内のイニシエータの OS タイプを選択します。
- [ポートセット（Port Set）] : ポート セットを入力します。

b) [送信（Submit）] をクリックします。

タスクの追加：イニシエータ グループへのイニシエータの追加

この手順は、例：iSCSI ブート ワークフローの作成，（33 ページ） に基づいてワークフローを作成済みで、オーケストレーション内に [ワークフロー（Workflow）] タブが表示されていることを前提としています。

手順

ステップ 1 左側のペインでワークフローがあるフォルダを展開し、タスクを追加する iSCSI ワークフローの行をクリックします。

ステップ 2 アイコンバーで紫のドロップダウン リスト アイコンをクリックして [ワークフローデザイナ（Workflow Designer）] を選択します。

ステップ 3 ワークフローデザイナの [使用可能なタスク（Available Tasks）] ペインで、[物理ストレージタスク（Physical Storage Tasks）] > [NetAppタスク（NetApp Tasks）] > [NetApp ONTAPタスク（NetApp ONTAP Tasks）] を展開します。

ステップ 4 [イニシエータグループへのイニシエータの追加] タスクをクリックし、選択したタスクをワークフロー デザイナ ウィンドウにドラッグ アンド ドロップします。

ステップ 5 [タスクの追加（イニシエータグループへのイニシエータの追加）] ウィザードの [タスク情報] 画面で、次の手順を実行します。

a) タスクを識別するタスク名とコメントを入力します。

b) エラーが発生した場合に、Cisco UCS Director でワークフローを自動的に再試行できるようにするには、次の手順を実行します。

- [再試行の実行（Retry Execution）] チェックボックスをオンにします。
- [再試行回数（Retry Count）] ドロップダウン リストから、再試行する回数を選択します。
- [再試行の頻度（Retry Frequency）] フィールドに、再試行間の秒数を示すコンマ区切りの値リストを入力します。

c) タスクの詳細を確認します。

d) [次へ（Next）] をクリックします。

ステップ 6 [タスクの追加（イニシエータグループへのイニシエータの追加）（Add Task (Add an Initiator to Initiator Group)）] ウィザードの [ユーザマッピング入力（User Mapping Inputs）] 画面で、次の手順を実行します。

a) ワークフロー実行時にボリュームの設定属性の一部を入力するプロンプトを表示したい場合は、次のチェックボックスの 1 つまたは複数をオンにして、ユーザ入力を選択します。

（注） ユーザ入力をマッピングするには、ワークフローにユーザ入力と適切な許可を追加する必要があります。

- [イニシエータグループ名（Initiator Group Name）]：イニシエータを追加するイニシエータ グループの名前を指定します。
- [イニシエータ名（Initiator Name）]：グループに追加するイニシエータを指定します。

b) [次へ（Next）] をクリックします。

ステップ 7 [タスクの追加（イニシエータグループへのイニシエータの追加）（Add Task (Add an Initiator to Initiator Group)）] ウィザードの [タスク入力（Task Inputs）] 画面で、次の手順を実行します。

a) ユーザ入力のプロンプトの表示を選択しなかったこれらの設定属性については、次の手順を実行します。

- [イニシエータグループ名（Initiator Group Name）]：イニシエータを追加するイニシエータ グループを選択します。
- [イニシエータ名（Initiator Name）]：グループに追加するイニシエータを入力します。複数のイニシエータを追加する場合は、名前をコンマで区切ります。
- [強制（Force）]：このチェックボックスをオンにすると、イニシエータがグループに強制的に追加されます。

b) [送信（Submit）] をクリックします。

タスクの追加：イニシエータ グループへの LUN のマッピング

この手順は、例：iSCSI ブート ワークフローの作成, （33 ページ） に基づいてワークフローを作成済みで、オーケストレーション内に [ワークフロー（Workflow）] タブが表示されていることを前提としています。

手順

ステップ 1 左側のペインでワークフローがあるフォルダを展開し、タスクを追加する iSCSI ワークフローの行をクリックします。

ステップ 2 アイコンバーで紫のドロップダウン リスト アイコンをクリックして [ワークフローデザイナ（Workflow Designer）] を選択します。

ステップ 3 ワークフローデザイナの [使用可能なタスク（Available Tasks）] ペインで、[物理ストレージタスク（Physical Storage Tasks）] > [NetAppタスク（NetApp Tasks）] > [NetApp ONTAPタスク（NetApp ONTAP Tasks）] を展開します。

ステップ 4 [イニシエータグループの作成（Create Initiator Group）] タスクをクリックし、選択したタスクをワークフロー デザイナ ウィンドウにドラッグ アンド ドロップします。

ステップ 5 [タスクの追加（イニシエータグループへのLUNのマッピング）] ウィザードの [タスク情報] 画面で、次の手順を実行します。

a) タスクを識別するタスク名とコメントを入力します。

b) エラーが発生した場合に、Cisco UCS Director でワークフローを自動的に再試行できるようにするには、次の手順を実行します。

- [再試行の実行（Retry Execution）] チェックボックスをオンにします。
- [再試行回数（Retry Count）] ドロップダウン リストから、再試行する回数を選択します。
- [再試行の頻度（Retry Frequency）] フィールドに、再試行間の秒数を示すコンマ区切りの値リストを入力します。

c) タスクの詳細を確認します。

d) [次へ（Next）] をクリックします。

ステップ 6 [タスクの追加（イニシエータグループへのLUNのマッピング）] ウィザードの [ユーザマッピング入力] 画面で、次の手順を実行します。

a) ワークフロー実行時にボリュームの設定属性の一部を入力するプロンプトを表示したい場合は、次のチェックボックスの 1 つまたは複数をオンにして、ユーザ入力を選択します。

（注） ユーザ入力をマッピングするには、ワークフローにユーザ入力と適切な許可を追加する必要があります。

- [ファイラID名（Filer Identity Name）] : イニシエータ グループのファイラを指定します。
- [イニシエータグループ名（Initiator Group Name）] : マッピングするイニシエータ グループの名前を指定します。
- [LUN ID] : イニシエータ グループにマッピングする LUN を指定します。
- [LUNパス（LUN Path）] : LUN へのファイル パスを指定します。

b) [次へ（Next）] をクリックします。

ステップ 7 [タスクの追加（イニシエータグループへのLUNのマッピング）] ウィザードの [タスク入力] 画面で、次の手順を実行します。

a) ユーザ入力のプロンプトの表示を選択しなかったこれらの設定属性については、次の手順を実行します。

- [ファイラID名（Filer Identity Name）] : イニシエータ グループのファイラを選択します。
- [イニシエータグループ名（Initiator Group Name）] : マッピングするイニシエータ グループの名前を選択します。
- [LUN ID] : このチェックボックスをオンにすると、先ほどワークフローで作成した LUN を指定できます。
- [LUNパス（LUN Path）] : LUN へのファイル パスを選択します。

b) [送信（Submit）] をクリックします。

タスクの追加：PXE ブートの設定

この手順は、例：iSCSI ブート ワークフローの作成，（33 ページ） に基づいてワークフローを作成済みで、オーケストレーション内に [ワークフロー（Workflow）] タブが表示されていることを前提としています。

手順

ステップ 1 左側のペインでワークフローがあるフォルダを展開し、タスクを追加する iSCSI ワークフローの行をクリックします。

ステップ 2 アイコンバーで紫のドロップダウン リスト アイコンをクリックして [ワークフローデザイナ（Workflow Designer）] を選択します。

ステップ 3 ワークフローデザイナの [使用可能なタスク（Available Tasks）] ペインで、[ネットワークサービスタスク（Network Services Tasks）] を展開します。

ステップ 4 [PXEブートの設定（Setup PXE Boot）] タスクをクリックし、選択したタスクをワークフローデザイナ ウィンドウにドラッグ アンド ドロップします。

ステップ 5 [タスクの追加（PXEブートの設定）（Add Task (Setup PXE Boot)）] ウィザードの [タスク情報（Task Information）] 画面で、次の手順を実行します。

a) タスクを識別するタスク名とコメントを入力します。

b) エラーが発生した場合に、Cisco UCS Director でワークフローを自動的に再試行できるようにするには、次の手順を実行します。

- [再試行の実行（Retry Execution）] チェックボックスをオンにします。
- [再試行回数（Retry Count）] ドロップダウン リストから、再試行する回数を選択します。
- [再試行の頻度（Retry Frequency）] フィールドに、再試行間の秒数を示すコンマ区切りの値リストを入力します。

c) タスクの詳細を確認します。

d) [次へ（Next）] をクリックします。

ステップ 6 [タスクの追加（PXEブートの設定）（Add Task (Setup PXE Boot)）] ウィザードの [ユーザマッピング入力（User Mapping Inputs）] 画面で、次の手順を実行します。

a) ワークフロー実行時にボリュームの設定属性の一部を入力するプロンプトを表示したい場合は、次のチェックボックスの 1 つまたは複数をオンにして、ユーザ入力を選択します。

（注） ユーザ入力をマッピングするには、ワークフローにユーザ入力と適切な許可を追加する必要があります。

- [サーバMACアドレス（Server MAC Address）]：PXE ブートを実行するサーバの MAC アドレスを指定します。複数のサーバを設定する場合は、コンマで区切って入力します。
- [サーバのIPアドレス（Server IP Address）]：サーバの IP アドレスを指定します。複数のサーバを設定する場合は、最初と最後の IP アドレスの間にハイフン（-）を入力するか、コンマで区切って入力します。

- [サーバネットマスク（Server Net Mask）]：PXE ブートに使用するネット マスクを指定します。
- [サーバホスト名（Server Host Name）]：サーバのホスト名を指定します。
- [サーバゲートウェイ（Server Gateway）]：PXE ブートに使用するゲートウェイを指定します。
- [ルートパスワード（Root Password）]：サーバのルート パスワードを指定します。
- [タイムゾーン（Timezone）]：サーバのタイム ゾーンを指定します。

b) [次へ（Next）] をクリックします。

ステップ 7 [タスクの追加（PXEブートの設定）（Add Task (Setup PXE Boot)）] ウィザードの [タスク入力（Task Inputs）] 画面で、次の手順を実行します。

a) ユーザ入力のプロンプトの表示を選択しなかったこれらの設定属性については、次の手順を実行します。

- [OSタイプ（OS Type）]：サーバの OS タイプを選択します。
- [サーバMACアドレス（Server MAC Address）]：PXE ブートを実行するサーバの MAC アドレスを入力します。複数のサーバを設定する場合は、コンマで区切って入力します。
- [サーバのIPアドレス]：サーバの IP アドレスを入力します。複数のサーバを設定する場合は、最初と最後の IP アドレスの間にハイフン（-）を入力するか、コンマで区切って入力します。
- [サーバネットマスク（Server Net Mask）]：PXE ブートに使用するネット マスクを入力します。
- [サーバホスト名（Server Host Name）]：サーバのホスト名を入力します。
- [サーバゲートウェイ（Server Gateway）]：PXE ブートに使用するゲートウェイを入力します。
- [サーバ名サーバ（Server Name Server）]：PXE ブートに使用するサーバ名を入力します。
- [管理VLAN（Management VLAN）]：PXE ブートに使用する VLAN を入力します。
- [ルートパスワード（Root Password）]：サーバのルート パスワードを入力します。
- [タイムゾーン（Timezone）]：サーバのタイム ゾーン選択します。

b) [送信（Submit）] をクリックします。

タスクの追加：UCS サーバの電源をオンにする

この手順は、例：iSCSI ブート ワークフローの作成，（33 ページ） に基づいてワークフローを作成済みで、オーケストレーション内に [ワークフロー（Workflow）] タブが表示されていることを前提としています。

手順

ステップ 1 左側のペインでワークフローがあるフォルダを展開し、タスクを追加する iSCSI ワークフローの行をクリックします。

ステップ 2 アイコンバーで紫のドロップダウン リスト アイコンをクリックして [ワークフローデザイナ（Workflow Designer）] を選択します。

ステップ 3 ワークフロー デザイナの [使用可能なタスク（Available Tasks）] ペインで [物理コンピューティング タスク（Physical Compute Tasks）] > [Cisco UCS タスク（Cisco UCS Tasks）] を展開します。

ステップ 4 [UCSサーバの電源をオンにする（Power On UCS Server）] タスクをクリックし、選択したタスクをワークフロー デザイナ ウィンドウにドラッグ アンド ドロップします。

ステップ 5 [タスクの追加（UCSサーバの電源をオンにする）（Add Task (Power On UCS Server)）] ウィザードの [タスク情報（Task Information）] 画面で、次の手順を実行します。

a) タスクを識別するタスク名とコメントを入力します。

b) エラーが発生した場合に、Cisco UCS Director でワークフローを自動的に再試行できるようにするには、次の手順を実行します。

- [再試行の実行（Retry Execution）] チェックボックスをオンにします。
- [再試行回数（Retry Count）] ドロップダウン リストから、再試行する回数を選択します。
- [再試行の頻度（Retry Frequency）] フィールドに、再試行間の秒数を示すコンマ区切りの値リストを入力します。

c) タスクの詳細を確認します。

d) [次へ（Next）] をクリックします。

ステップ 6 [タスクの追加（UCSサーバの電源をオンにする）（Add Task (Power On UCS Server)）] ウィザードの [ユーザマッピング入力（User Mapping Inputs）] 画面で、次の手順を実行します。

a) ワークフロー実行時に電源をオンにするサーバを指定するプロンプトを表示したい場合は、[サーバ（Server）] チェックボックスをオンにして、ユーザ入力を選択します。

b) [次へ（Next）] をクリックします。

ステップ 7 [タスクの追加（UCSサーバの電源をオンにする）（Add Task (Power On UCS Server)）] ウィザードの [タスク入力（Task Inputs）] 画面で、次の手順を実行します。

a) ユーザ入力のプロンプトの表示を選択しなかった場合は、[サーバ（Server）] ドロップダウン リストから電源をオンにしたいサーバを選択します。

b) [送信（Submit）] をクリックします。

タスクの追加：PXE ブートのモニタリング

この手順は、例：iSCSI ブート ワークフローの作成, （33 ページ） に基づいてワークフローを作成済みで、オーケストレーション内に [ワークフロー（Workflow）] タブが表示されていることを前提としています。

手順

ステップ 1 左側のペインでワークフローがあるフォルダを展開し、タスクを追加する iSCSI ワークフローの行をクリックします。

ステップ 2 アイコンバーで紫のドロップダウン リスト アイコンをクリックして [ワークフローデザイナ（Workflow Designer）] を選択します。

ステップ 3 ワークフローデザイナの [使用可能なタスク（Available Tasks）] ペインで、[ネットワークサービス タスク（Network Services Tasks）] を展開します。

ステップ 4 [PXEブートのモニタリング（Monitor PXE Boot）] タスクをクリックし、選択したタスクをワークフロー デザイナ ウィンドウにドラッグ アンド ドロップします。

ステップ 5 [タスクの追加（PXEブートのモニタリング）（Add Task (Monitor PXE Boot)）] ウィザードの [タスク情報（Task Information）] 画面で、次の手順を実行します。

a) タスクを識別するタスク名とコメントを入力します。

b) エラーが発生した場合に、Cisco UCS Director でワークフローを自動的に再試行できるようにするには、次の手順を実行します。

- [再試行の実行（Retry Execution）] チェックボックスをオンにします。
- [再試行回数（Retry Count）] ドロップダウン リストから、再試行する回数を選択します。
- [再試行の頻度（Retry Frequency）] フィールドに、再試行間の秒数を示すコンマ区切りの値リストを入力します。

c) タスクの詳細を確認します。

d) [次へ（Next）] をクリックします。

ステップ 6 [タスクの追加（PXEブートのモニタリング）（Add Task (Monitor PXE Boot)）] ウィザードの [ユーザマッピング入力（User Mapping Inputs）] 画面で、次の手順を実行します。

a) ワークフロー実行時に PXE 要求 ID を入力するプロンプトを表示したい場合は、[PXE要求ID（PXE Request ID）] チェックボックスをオンにして、ユーザ入力を選択します。

（注） ユーザ入力をマッピングするには、ワークフローにユーザ入力と適切な許可を追加する必要があります。

b) [次へ（Next）] をクリックします。

ステップ 7 [タスクの追加（PXEブートのモニタリング）（Add Task (Monitor PXE Boot)）] ウィザードの [タスク入力（Task Inputs）] 画面で、次の手順を実行します。

a) ユーザ入力のプロンプトの表示を選択しなかったこれらの設定属性については、次の手順を実行します。

- [PXE要求ID（PXE Request ID）]：PXE要求ID を入力します。
- [最大待機時間（Max Wait Time）]：PXE ブートが完了するまでの最大待機時間を選択します。

b) [送信（Submit）] をクリックします。

タスクの追加：UCS サーバの電源をオフにする

この手順は、例：iSCSI ブート ワークフローの作成，（33 ページ） に基づいてワークフローを作成済みで、オーケストレーション内に [ワークフロー（Workflow）] タブが表示されていることを前提としています。

手順

ステップ 1 左側のペインでワークフローがあるフォルダを展開し、タスクを追加する iSCSI ワークフローの行をクリックします。

ステップ 2 アイコンバーで紫のドロップダウン リスト アイコンをクリックして [ワークフローデザイナ（Workflow Designer）] を選択します。

ステップ 3 ワークフロー デザイナの [使用可能なタスク（Available Tasks）] ペインで [物理コンピューティング タスク（Physical Compute Tasks）] > [Cisco UCS タスク（Cisco UCS Tasks）] を展開します。

ステップ 4 [UCSサーバの電源をオフにする（Power Off UCS Server）] タスクをクリックし、選択したタスクをワークフロー デザイナ ウィンドウにドラッグ アンド ドロップします。

ステップ 5 [タスクの追加（UCSサーバの電源をオフにする）（Add Task (Power Off UCS Server)）] ウィザードの [タスク情報（Task Information）] 画面で、次の手順を実行します。

a) タスクを識別するタスク名とコメントを入力します。

b) エラーが発生した場合に、Cisco UCS Director でワークフローを自動的に再試行できるようにするには、次の手順を実行します。

- [再試行の実行（Retry Execution）] チェックボックスをオンにします。
- [再試行回数（Retry Count）] ドロップダウン リストから、再試行する回数を選択します。
- [再試行の頻度（Retry Frequency）] フィールドに、再試行間の秒数を示すコンマ区切りの値リストを入力します。

c) タスクの詳細を確認します。

d) [次へ（Next）] をクリックします。

ステップ 6 [タスクの追加（UCSサーバの電源をオフにする）（Add Task (Power Off UCS Server)）] ウィザードの [ユーザマッピング入力（User Mapping Inputs）] 画面で、次の手順を実行します。

a) ワークフロー実行時に電源をオフにするサーバを指定するプロンプトを表示したい場合は、[サーバ（Server）] チェックボックスをオンにして、ユーザ入力を選択します。

b) [次へ（Next）] をクリックします。

ステップ 7 [タスクの追加（UCSサーバの電源をオフにする）（Add Task (Power Off UCS Server)）] ウィザードの [タスク入力（Task Inputs）] 画面で、次の手順を実行します。

a) ユーザ入力のプロンプトの表示を選択しなかった場合は、[サーバ（Server）] ドロップダウン リストから電源をオフにしたいサーバを選択します。

b) [送信（Submit）] をクリックします。

タスクの追加：iSCSI からブートするためのサービス プロファイル ブート ポリシーの変更

この手順は、例：iSCSI ブート ワークフローの作成, （33 ページ） に基づいてワークフローを作成済みで、オーケストレーション内に [ワークフロー（Workflow）] タブが表示されていることを前提としています。

手順

ステップ 1 左側のペインでワークフローがあるフォルダを展開し、タスクを追加する iSCSI ワークフローの行をクリックします。

ステップ 2 アイコンバーで紫のドロップダウン リスト アイコンをクリックして [ワークフローデザイナ（Workflow Designer）] を選択します。

ステップ 3 ワークフロー デザイナの [使用可能なタスク（Available Tasks）] ペインで [物理コンピューティング タスク（Physical Compute Tasks）] > [Cisco UCS タスク（Cisco UCS Tasks）] を展開します。

ステップ 4 [iSCSIからブートするためのサービスプロファイルのブートポリシーの変更（Modify Service Profile Boot Policy to Boot from iSCSI）] タスクをクリックし、選択したタスクをワークフロー デザイナ ウィンドウにドラッグ アンド ドロップします。

ステップ 5 [タスクの追加（iSCSIからブートするためのサービスプロファイルのブートポリシーの変更）（Add Task (Modify Service Profile Boot Policy to Boot from iSCSI)）] ウィザードの [タスク情報（Task Information）] 画面で、次の手順を実行します。

a) タスクを識別するタスク名とコメントを入力します。

b) エラーが発生した場合に、Cisco UCS Director でワークフローを自動的に再試行できるようにするには、次の手順を実行します。

- [再試行の実行（Retry Execution）] チェックボックスをオンにします。
- [再試行回数（Retry Count）] ドロップダウン リストから、再試行する回数を選択します。
- [再試行の頻度（Retry Frequency）] フィールドに、再試行間の秒数を示すコンマ区切りの値リストを入力します。

c) タスクの詳細を確認します。

d) [次へ（Next）] をクリックします。

ステップ 6 [タスクの追加（iSCSIからブートするためのサービスプロファイルのブートポリシーの変更）（Add Task (Modify Service Profile Boot Policy to Boot from iSCSI)）] ウィザードの [ユーザマッピング入力（User Mapping Inputs）] 画面で、次の手順を実行します。

a) ワークフロー実行時に変更するサービス プロファイルを指定するプロンプトを表示したい場合は、[サービス プロファイル（Service Profile）] チェックボックスをオンにして、ユーザ入力を選択します。

b) [次へ（Next）] をクリックします。

ステップ 7 [タスクの追加（iSCSIからブートするためのサービスプロファイルのブートポリシーの変更）（Add Task (Modify Service Profile Boot Policy to Boot from iSCSI)）] ウィザードの [タスク入力（Task Inputs）] 画面で、次の手順を実行します。

a) ユーザ入力のプロンプトの表示を選択しなかった場合は、[サービス プロファイル（Service Profile）] ボタンをクリックして変更するサービス プロファイルを選択します。

b) [送信（Submit）] をクリックします。

ブート ポリシーのブート順の変更

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 ポリシーを変更する組織をクリックし、[詳細の表示（View Details）] をクリックします。

ステップ 5 [ブート ポリシー（Boot Policies）] をクリックします。

ステップ 6 複製するブート ポリシーを選択し、[ブートデバイスの順序の管理（Manage Boot Devices Order）] をクリックします。

ステップ 7 次のボタンを使用して、ブート デバイスの順序を変更します。

- [上に移動（Move Up）]
- [下に移動（Move Down）]
- [削除（Delete）]

ステップ 8 完了したら、[戻る（Back）] をクリックします。

ローカル ディスク設定ポリシー

このポリシーは、ローカル ドライブのオンボード RAID コントローラを通じて、サーバ上にインストールされているオプションの SAS ローカル ドライブを設定します。このポリシーでは、ローカルディスク設定ポリシーを含むサービスプロファイルに関連付けられたすべてのサーバに対して、ローカル ディスク モードを設定できるようにします。

ローカル ディスク モードには次のものがあります。

- [ローカルストレージなし（No Local Storage）]：ディスクレス サーバまたは SAN 専用の設定で使用します。このオプションを選択する場合、このポリシーを使用する任意のサービス プロファイルを、ローカル ディスクを持つサーバに関連付けることができません。
- [RAID 0がストライプ済み（RAID 0 Striped）]：データはアレイのすべてのディスクにストライプ化され、高速スループットを提供します。 データの冗長性はなく、いずれかのディスクで障害が発生すると、すべてのデータが失われます。
- [RAID 1がミラー済み（RAID 1 Mirrored）]：データが 2 つのディスクに書き込まれ、1 つのディスクで障害が発生した場合でも完全なデータ冗長性を提供します。最大アレイ サイズは、2 つのドライブの小さい方の空き容量に等しくなります。
- [任意の設定（Any Configuration）]：変更なしのローカル ディスク設定を転送するサーバ設定で使用します。
- [RAIDなし（No RAID）]：RAID を削除し、ディスク MBR およびペイロードを変更しない状態のままにするサーバ設定で使用します。

  [RAIDなし（No RAID）] を選択し、このポリシーをすでに RAID ストレージが設定されているオペレーティング システムを使用するサーバに適用した場合、ディスクの内容は削除されません。そのため、[RAIDなし（No RAID）] モードの適用後にサーバでの違いがわからないことがあります。よって、ポリシーの RAID 設定と、サーバの [インベントリ（Inventory）] > [ストレージ（Storage）] タブに表示される実際のディスク設定とが一致しない場合があります。

  以前のすべての RAID 設定情報をディスクから削除するには、[RAIDなし（No RAID）] コンフィギュレーション モードの適用後にすべてのディスク情報を削除するスクラブ ポリシーを適用します。
- [RAID 5が部分的にストライプ済み（RAID 5 Striped Parity）]：データはアレイのすべてのディスクにストライプ化されます。 各ディスクの容量の一部に、ディスクの障害発生時にデータの再構築に使用できるパリティ情報が格納されます。RAID 5 は、高い読み取り要求レートで、アプリケーションに適切なデータ スループットを提供します。
- [RAID 6が部分的にデュアルストライプ済み（RAID 6 Striped Dual Parity）]：データはアレイのすべてのディスクにストライプ化され、2 つのパリティ ディスクを使用して、最大 2 つの物理ディスクの障害に対する保護を提供します。データ ブロックの各行に、2 セットのパリティ データが格納されます。

- [RAID 10がミラーおよびストライプ済み（RAID 10 Mirrored and Striped）]：RAID 10はミラー化されたディスクのペアを使用して、完全なデータ冗長性と高いスループット レートを提供します。
- [RAID 50が部分的にストライプおよびストライプ済み]：データが複数のストライプ化されたパリティ ディスク セットにストライプ化され、高いスループットと複数のディスク故障耐性を提供します。
- [RAID 60部分的にストライプおよびストライプ済み]：データが複数のストライプ化されたパリティ ディスク セットにストライプ化され、高いスループットと優れたディスク故障耐性を提供します。

このポリシーはサービス プロファイルに組み込む必要があります。また。このポリシーを有効にするには、サーバに関連付ける必要があります。

（注） 組み込みオンボードRAIDコントローラを搭載したCisco UCS Managerと統合されたCisco UCS Cシリーズ サーバの場合、ローカル ディスク モードは常に[任意の設定（Any Configuration）]でなければならず、RAIDはコントローラ上で直接設定する必要があります。

すべてのローカル ディスク設定ポリシーに関するガイドライン

ローカル ディスク設定ポリシーを作成する前に、次のガイドラインを考慮してください。

HDD と SSD を混合しない

1 台のサーバや RAID 設定に、HDD と SSD を使用しないでください。

B200 M1 または M2 のデフォルト ローカル ディスク設定ポリシーを使用して、B200 M3 にサービス プロファイルを割り当てない

B200 M1 および M2 サーバと B200 M3 サーバのストレージ コントローラで提供される RAID/JBOD サポートは異なっているため、B200M1 または M2 サーバのデフォルト ローカル ディスク設定ポリシーを含むサービス プロファイルを B200 M3 サーバに割り当てたり、再割り当てを行ったりすることはできません。デフォルトのローカル ディスク設定ポリシーには、[任意の設定（Any Configuration）] モードまたは JBOD 設定が含まれます。

JBOD モードのサポート

B200 M3 サーバでは、ローカル ディスクの JBOD モードがサポートされています。

（注） ローカル ディスクの JBOD モードをサポートしているのは、B200 M1、B200 M2、B200 M3、B250 M1、B250 M2、B22 M3 ブレード サーバのみです。

RAID 用に設定されているローカル ディスク設定ポリシーに関するガイドライン

MegaRAID ストレージ コントローラを搭載したサーバ用のローカル ディスク設定ポリシーに RAID 設定を設定する

ブレード サーバまたは統合されたラックマウント サーバに MegaRAID コントローラが搭載されている場合、そのサーバのサービスプロファイルに含まれるローカルディスク設定ポリシーでドライブの RAID 設定を設定する必要があります。これを実行するには、そのサーバに定義されている RAID モードのいずれかを使用して、サービス プロファイルのローカル ディスク設定ポリシーを設定するか、[任意の設定（Any Configuration）] モードと LSI ユーティリティ ツールセットを使用して、RAID ボリュームを作成します。

OS をインストールする前に RAID LUN を設定していないと、インストール時にディスク検出エラーが発生し、「No Device Found」といったエラー メッセージが表示される可能性があります。

サーバ プロファイルで [任意の設定（Any Configuration）] モードが指定されている場合、RAID 1 クラスタ移行後にサーバが起動しない

RAID 1 クラスタの移行後、サービス プロファイルをサーバに関連付ける必要があります。サービス プロファイル内のローカル ディスク設定ポリシーに [RAID 1] ではなく [任意の設定（Any Configuration）] モードが設定されていると、RAID LUN は、関連付け中およびその後も「非アクティブ」状態のままになります。その結果、サーバは起動できなくなります。

この問題を回避するには、サーバに関連付けるサービス プロファイルに、移行前の元のサービス プロファイルとまったく同じローカル ディスク設定ポリシーが含まれるようにし、[任意の設定（Any Configuration）] モードは含まれないようにします。

MegaRAID ストレージ コントローラを搭載したサーバ上で JBOD モードを使用しない

MegaRAID ストレージコントローラが搭載されたブレードサーバまたは統合ラックマウント サーバ上で JBOD モードまたは JBOD 操作を設定または使用しないでください。JBOD モードと操作は、このサーバで完全に機能するよう設計されていません。

統合されたラックマウント サーバ内の RAID ボリュームと RAID コントローラはそれぞれ 1 つまで

Cisco UCS Manager と統合されているラックマウント サーバは、Cisco UCS Centralサーバ上に存在するハード ドライブの数とは関係なく、RAID ボリュームを 1 つまでしか設定できません。

統合されたラックマウント サーバ内のローカル ハード ドライブは、1 つの RAID コントローラのみにすべて接続される必要があります。Cisco UCS Manager との統合では、ローカル ハード ドライブが単一のラックマウント サーバ内の複数の RAID コントローラに接続することはサポートされていません。そのため、Cisco UCS Manager と統合されるラックマウント サーバを発注する際は、単一の RAID コントローラ構成を要求することを推奨します。

また、サードパーティ製のツールを使用して、ラックマウント サーバ上に複数の RAID LUN を作成しないでください。Cisco UCS Manager では、そのような設定はサポートされていません。

ブレード サーバ内の RAID ボリュームと RAID コントローラはそれぞれ 1 つまで

ブレード サーバは、サーバ内に存在するドライブの数とは関係なく、RAID ボリュームを 1 つまでしか設定できません。ローカル ハード ドライブは、1 つの RAID コントローラのみにすべて接続される必要があります。たとえば、B200 M3 に LSI コントローラと Intel Patsburg コントローラが搭載されていても、LSI コントローラだけが RAID コントローラして使用できます。

また、サードパーティ製のツールを使用して、ブレード サーバ上に複数の RAID LUN を作成しないでください。Cisco UCS Manager では、そのような設定はサポートされていません。

ミラー RAID で選択されるディスクの数は 2 つまでにする

ミラー RAID で選択されたディスクの数が 2 つを超えると、RAID 1 は RAID 10 LUN として作成されます。この問題は、Cisco UCS B440 M1 サーバと B440 M2 サーバで発生する可能性があります。

一部のサーバの特定の RAID 設定オプションでは、ライセンスが必要

一部の Cisco UCS サーバには、特定の RAID 設定オプションのライセンスが必要です。Cisco UCS Manager で、このローカル ディスク ポリシーを含むサービス プロファイルとサーバを関連付けると、Cisco UCS Manager によって選択された RAID オプションに適切なライセンスが備わっているかが確認されます。問題がある場合は、サービス プロファイルを関連付ける際に、Cisco UCS Manager に設定エラーが表示されます。

特定の Cisco UCS サーバの RAID ライセンス情報については、そのサーバの『*Hardware Installation Guide*』を参照してください。

B420 M3 サーバでは全コンフィギュレーション モードはサポートされていない

B420 M3 サーバでは、ローカル ディスク設定ポリシーで、次のような設定オプションはサポートされていません。

- RAID なし
- RAID 6 ストライプ化デュアルパリティ

また、B420 M3 では JBOD モードや操作はサポートされていません。

シングル ディスク RAID 0 設定は、一部のブレード サーバではサポートされていない

シングル ディスク RAID 0 設定は、次のブレード サーバではサポートされていません。

- Cisco UCS B200 M1
- Cisco UCS B200 M2
- Cisco UCS B250 M1
- Cisco UCS B250 M2

ローカル ディスク設定ポリシーの作成

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 ポリシーを作成する組織をクリックして [詳細の表示（View Details）] をクリックします。

ステップ 5 [ローカル ディスクの設定ポリシー（Local Disk Configuration Policies）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [ローカル ディスクの設定ポリシー（Local Disk Configuration Policy）] 画面で、次の手順を実行します。

a) [名前（Name）] フィールドに、ポリシーの一意の名前を入力します。

b) [説明（Description）] フィールドに、ポリシーの説明を入力します。
ポリシーが使用される場所と条件についての情報を含めることを推奨します。

c) [モード（Mode）] ドロップダウン リストから、次のローカルディスク ポリシー モードのいずれかを選択します。

- [ローカルストレージなし（No Local Storage）] : ディスクレス サーバまたは SAN 専用の設定で使用します。このオプションを選択する場合、このポリシーを使用する任意のサービス プロファイルを、ローカル ディスクを持つサーバに関連付けることができません。
- [RAID 0がストライプ済み（RAID 0 Striped）] : データはアレイのすべてのディスクにストライプ化され、高速スループットを提供します。 データの冗長性はなく、いずれかのディスクで障害が発生すると、すべてのデータが失われます。
- [RAID 1がミラー済み（RAID 1 Mirrored）] : データが 2 つのディスクに書き込まれ、1 つのディスクで障害が発生した場合でも完全なデータ冗長性を提供します。最大アレイ サイズは、2 つのドライブの小さい方の空き容量に等しくなります。
- [任意の設定（Any Configuration）] : 変更なしのローカル ディスク設定を転送するサーバ設定で使用します。
- [RAIDなし（No RAID）] : RAID を削除し、ディスク MBR およびペイロードを変更しない状態のままにするサーバ設定で使用します。

  [RAIDなし（No RAID）] を選択し、このポリシーをすでに RAID ストレージが設定されているオペレーティング システムを使用するサーバに適用した場合、ディスクの内容は削除されません。そのため、[RAIDなし（No RAID）] モードの適用後にサーバでの違いがわからないことがあります。よって、ポリシーの RAID 設定と、サーバの [インベントリ（Inventory）] > [ストレージ（Storage）] タブに表示される実際のディスク設定とが一致しない場合があります。

以前のすべての RAID 設定情報をディスクから削除するには、[RAIDなし（No RAID）] コンフィギュレーション モードの適用後にすべてのディスク情報を削除するスクラブ ポリシーを適用します。

- [RAID 5が部分的にストライプ済み（RAID 5 Striped Parity）]：データはアレイのすべてのディスクにストライプ化されます。 各ディスクの容量の一部に、ディスクの障害発生時にデータの再構築に使用できるパリティ情報が格納されます。RAID 5 は、高い読み取り要求レートで、アプリケーションに適切なデータ スループットを提供します。
- [RAID 6が部分的にデュアルストライプ済み（RAID 6 Striped Dual Parity）]：データはアレイのすべてのディスクにストライプ化され、2 つのパリティ ディスクを使用して、最大 2 つの物理ディスクの障害に対する保護を提供します。データ ブロックの各行に、2 セットのパリティ データが格納されます。
- [RAID 10がミラーおよびストライプ済み（RAID 10 Mirrored and Striped）]：RAID 10 はミラー化されたディスクのペアを使用して、完全なデータ冗長性と高いスループット レートを提供します。
- [RAID 50が部分的にストライプおよびストライプ済み]：データが複数のストライプ化されたパリティ ディスク セットにストライプ化され、高いスループットと複数のディスク故障耐性を提供します。
- [RAID 60部分的にストライプおよびストライプ済み]：データが複数のストライプ化されたパリティ ディスク セットにストライプ化され、高いスループットと優れたディスク故障耐性を提供します。

（注） 一部の Cisco UCS サーバには、特定の RAID 設定オプションのライセンスが必要です。Cisco UCS Manager で、このローカルディスク ポリシーを含むサービス プロファイルとサーバを関連付けると、Cisco UCS Manager によって選択された RAID オプションに適切なライセンスが備わっているかが確認されます。問題がある場合は、サービス プロファイルを関連付ける際に、Cisco UCS Manager に設定エラーが表示されます。

特定の Cisco UCS サーバの RAID ライセンス情報については、そのサーバの『*Hardware Installation Guide*』を参照してください。

d) サーバとサービスプロファイルとの関連が解除されても、このローカルディスク設定ポリシーを保持したい場合は、[設定の保護（Protect Configuration）] チェックボックスをオンにします。

注意 サーバ内の 1 つ以上のディスクに障害が発生すると、[設定の保護（Protect Configuration）] は機能しなくなります。

このプロパティは、デフォルトでオンになっています。

サービス プロファイルがサーバから関連付けを解除され、新しいサービス プロファイルが関連付けられると、新しいサービス プロファイルの Protect Configuration プロパティの設定が優先され、前のサービス プロファイルの設定が上書きされます。

（注） このオプションが有効な状態でサーバとサービス プロファイルの関連付けを解除した後、そのサーバに新しいサービス プロファイルを関連付け、そのサービス プロファイル内のローカル ディスク設定ポリシーに前とは異なるプロパティが含まれていると、サーバから設定不一致のエラーが返され、関連付けは失敗します。

e) [Flex Flashの状態（Flex Flash State）] ドロップダウン リストから、SD カード モジュールを有効にするか無効にするかを選択します。
（注） このパラメータは、SD カード モジュールのあるサーバのみ該当します。
f) [送信（Submit）] をクリックします。

次の作業

ポリシーをサービス プロファイルまたはサービス プロファイル テンプレートに含めます。

メンテナンス ポリシー

メンテナンス ポリシーは、以下に変更が加えられた場合に、サーバの再起動に対して Cisco UCS Director がどの種類の要求を Cisco UCS Manager に送信するかを決定します。

- サーバに関連付けられているサービス プロファイル
- または、更新テンプレートにバインドされているサービス プロファイル。

メンテナンスポリシーは、サービスプロファイルの変更の展開方法を指定します。展開は、次のいずれかの方法で実行されます。

- 即時
- ユーザが管理者権限で承認したときに実行する
- スケジュールで指定された時間に自動的に実行する

スケジュール済みのメンテナンス ウィンドウ中に変更を展開するように設定されているメンテナンス ポリシーでは、ポリシーに有効なスケジュールが含まれていることが必要です。この場合、最初に使用可能なメンテナンス ウィンドウ中に変更が展開されます。

ユーザの確認応答を適用するには、Cisco UCS Manager の保留アクティビティ レポートの表示とユーザの確認応答 を参照してください。

（注） メンテナンス ポリシーでは、関連付けられたサービス プロファイルに設定変更が加えられた場合に、サーバの即時リブートは回避できますが、次のアクションの即時実行は回避されません。

- 関連付けられたサービス プロファイルのシステムからの削除
- サーバ プロファイルのサーバからの関連付けの解除
- サービス ポリシーを使用しないファームウェア アップグレードの直接インストール
- サーバのリセット

メンテナンスポリシー、およびサービスプロファイルの変更のインポートに関するガイドラインを含む遅延展開の詳細については、『Cisco UCS Manager configuration guides』を参照してください。

メンテナンス ポリシーの作成

はじめる前に

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 ポリシーを作成する組織をクリックして [詳細の表示（View Details）] をクリックします。

ステップ 5 [メンテナンス ポリシー（Maintenance Policies）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [メンテナンス ポリシーの作成（Create Maintenance Policy）] 画面で、次のフィールドに値を入力します。

名前	説明
[名前（Name）] フィールド	ポリシーの一意の名前。
[説明（Description）] フィールド	ポリシーの説明。ポリシーが使用される場所と条件についての情報を含めることを推奨します。

名前	説明
[リブートポリシー（Reboot Policy）] ドロップダウン リスト	このメンテナンスポリシーの含まれるサービスプロファイルと関連付けられたサーバで、リブートを発生させるタイミングを選択します。次のいずれかになります。 • [自動タイマー（Timer Automatic）]：サービス プロファイルのすべての関連付けと変更が、[スケジュール（Schedule）]フィールドに表示されたスケジュールで定義されているメンテナンス ウィンドウまで延期されます。 • [即時（Immediate）]：サービス プロファイルの関連付けが完了したり、サービス プロファイルの変更がユーザによって保存されるとすぐに、自動的にリブートが実行されます。 • [ユーザ認識（User Ack）]：サービス プロファイルの関連付けが完了したり、変更が行われたりした後に、ユーザがサーバを手動でリブートする必要があります。 手動の確認応答については、Cisco UCS Manager の保留アクティビティ レポートの表示とユーザの確認応答 を参照してください。
[スケジュール（Schedule）] ドロップダウン リスト	サービスプロファイルの関連付けや変更などのメンテナンス操作を実行するスケジュールを選択します。設定された期間中に、メンテナンスポリシーを含むサービスプロファイルと関連付けられたサーバがリブートされ、サービスプロファイルのすべての変更が完了します。 このフィールドは、[リブートポリシー（Reboot Policy）] が [自動タイマー（Timer Automatic）] に設定されている場合にのみ使用できます。スケジュールによって、サーバのメンテナンス操作が適用されるタイミングを指定できます。

ステップ 8 [送信（Submit）] をクリックします。

次の作業

ポリシーをサービス プロファイルまたはサービス プロファイル テンプレートに含めます。

サーバ プール ポリシー資格情報の概要

このポリシーは、ディスカバリ プロセス中に実行されたサーバのインベントリに基づいて、サーバを資格認定します。資格情報は、サーバが選択基準を満たすかどうかを判断するために、ポリシーで設定されたルールです。たとえば、データセンター プールのサーバの最小メモリ容量を指定するルールを作成できます。

資格情報は、サーバプールポリシーだけではなく、その他のポリシーでも、サーバを配置するために使用されます。たとえば、サーバがある資格ポリシーの基準を満たしている場合、このサーバを1つ以上のサーバプールに追加したり、自動的にサービス プロファイルと関連付けたりできます。

サーバ プール ポリシー資格情報を使用すると、次の基準に従ってサーバを資格認定できます。

- アダプタのタイプ
- シャーシの場所
- メモリのタイプと設定
- 電源グループ
- CPU のコア数、タイプ、および設定
- ストレージの設定と容量
- サーバのモデル

実装によっては、サーバプールポリシー資格情報を使用して、次を含む複数のポリシーを設定する必要があります。

- 自動構成ポリシー
- シャーシ ディスカバリ ポリシー
- サーバ ディスカバリ ポリシー
- サーバ継承ポリシー
- サーバ プール ポリシー

サーバ プール ポリシーの資格情報の作成

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 ポリシーを作成する組織をクリックして [詳細の表示（View Details）] をクリックします。

ステップ 5 [サーバ プール ポリシー資格情報（Server Pool Policy Qualifications）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [サーバ プール ポリシー認定の作成（Create Server Pool Policy Qualifications）] 画面で、ポリシーの名前と説明を入力し、[次へ（Next）] をクリックします。

ステップ 8 [アダプタの条件（Adapter Qualifications）] ページで、次の手順を実行してアダプタの条件をポリシーに追加するか、それらを追加しない場合は [次へ（Next）] をクリックします。

a) [アダプタの条件の追加（Add Adapter Qualifications）] チェックボックスをオンにします。

b) [タイプ（Type）] ドロップダウンリストから、ポリシーに含めるアダプタのタイプを選択します。
アダプタの条件を保存すると、このタイプは変更できなくなります。

c) [モデル(正規表現)（Model(RegEx)）] フィールドに、アダプタ PID が一致する必要のある正規表現を入力します。

d) [最大容量を入力（Maximum Capacity）] フィールドに、選択したタイプの最大容量を入力します。

e) [次へ（Next）] をクリックします。

ステップ 9 [シャーシ認定またはサーバ認定（Chassis/Server Qualifications）] ページで、次の手順を実行してシャーシ認定およびサーバ認定をポリシーに追加するか、それらを追加しない場合は [次へ（Next）] をクリックします。

a) [シャーシ認定またはサーバ認定の追加（Add Chassis/Server Qualifications）] チェックボックスをオンにします。

b) [最初のシャーシID（First Chassis ID）] フィールドに、このポリシーに関連付けられているサーバ プールが取得できる最初のシャーシ ID を入力します。
アダプタの条件を保存すると、このタイプは変更できなくなります。

c) [シャーシ数（Number of Chassis）] フィールドに、プールに含めるシャーシの合計数を入力します。この場合、[最初のシャーシID（First Chassis ID）] フィールドで指定したシャーシから数え始めます。

d) [サーバ認定の範囲（Server Qualification Ranges）] フィールドに、使用するサーバの位置の範囲を入力します。
複数の範囲を入力する場合は、範囲をカンマで区切ります。たとえば、1:5,2:6 と入力します。

e) [次へ（Next）] をクリックします。

例：
たとえば、シャーシ 5、6、7、8 を使用する場合、[最初のシャーシID（First Chassis ID）] フィールドに 5 を入力し、[シャーシ数（Number of Chassis）] フィールドに 4 を入力します。シャーシ 3 のみを使用する場合は、[最初のシャーシID（First Chassis ID）] フィールドに 3 を入力し、[シャーシ数（Number of Chassis）] フィールドに 1 を入力します。

ステップ 10 [メモリ認定（Memory Qualifications）] ページで、次の手順を実行してメモリ認定をポリシーに追加するか、それらを追加しない場合は [次へ（Next）] をクリックします。

a) [メモリ認定の追加（Add Memory Qualifications）] チェックボックスをオンにします。

b) 次のフィールドに入力します。

名前	説明
[クロック（Clock）]フィールド	必要な最小クロック速度（MHz）。
[最小容量（Min Cap）] フィールド	最小限必要なメモリ容量（メガバイト単位）。
[最大容量（Max Cap）]フィールド	メモリの許容最大容量（メガバイト単位）。
[幅（Width）] フィールド	データ バスの最小幅。
[遅延（Latency）] フィールド	許容される最大遅延（ナノ秒）。
[ユニット（Units）] フィールド	[幅（Width）] フィールドの値と関連付けられる測定単位。

c) [次へ（Next）] をクリックします。

ステップ 11 [CPU 認定またはコア認定（CPU/Cores Qualifications）] ページで、次の手順を実行して CPU 認定およびコア認定をポリシーに追加するか、それらを追加しない場合は [次へ（Next）] をクリックします。

a) [CPU認定またはコア認定の追加（Add CPU/Cores Qualifications）] チェックボックスをオンにします。

b) 次のフィールドに入力します。

名前	説明
[プロセッサアーキテクチャ（Processor Architecture）] ドロップダウン リスト	このポリシーが適用される CPU アーキテクチャを選択します。
[コアの最小数（Min Number of Cores）] フィールド	最小限必要な CPU コアの数。1 ～ 65535 の整数を指定します。

名前	説明
[コアの最大数（Max Number of Cores）] フィールド	CPU コアの許容最大数。1 ～ 65535 の整数を指定します。
[スレッドの最小数（Min Number of Threads）] フィールド	最小限必要なCPUスレッドの数。関連付けられたテキスト フィールドで 1 ～ 65535 の整数を指定します。
[スレッドの最大数（Max Number of Threads）] フィールド	CPU スレッドの許容最大数。1 ～ 65535 の整数を指定します。
[CPU速度（CPU Speed）] フィールド	最小限必要な CPU 速度。
[モデル(正規表現)（Model(RegEx)）] フィールド	プロセッサ PID が一致する必要のある正規表現。
[CPUステッピング（CPU Stepping）] フィールド	最小限必要な CPU バージョン。

c) [次へ（Next）] をクリックします。

ステップ 12 [ストレージ認定（Storage Qualifications）] ページで、次の手順を実行してストレージ認定をポリシーに追加するか、それらを追加しない場合は [次へ（Next）] をクリックします。

a) [ストレージ認定の追加（Add Storage Qualifications）] チェックボックスをオンにします。

b) 次のフィールドに入力します。

名前	説明
[ディスクレス（Diskless）] ドロップダウン リスト	使用可能なストレージをディスクレスにする必要があるかどうかを選択します。次のいずれかを選択できます。 • [未指定（Unspecified）] : どのストレージ タイプも受け入れ可能です。 • [はい（Yes）] : ストレージタイプはディスクレスにする必要があります。 • [いいえ（No）] : ストレージをディスクレスにすることはできません。 [はい（Yes）]を選択した場合、追加のフィールドは表示されません。
[最小容量（Min Cap）] フィールド	サーバ内のすべてのディスクの最小ストレージ容量（メガバイト単位）。

名前	説明
[最大容量（Max Cap）] フィールド	ストレージの許容最大容量（メガバイト単位）。
[ブロック数（Number of Blocks）] フィールド	最小限必要なブロック数。
[各ディスクの容量（Per Disk Cap）] フィールド	最小限必要なディスクあたりのストレージ容量（ギガバイト単位）。
[ブロック サイズ（Block Size）] フィールド	最小限必要なブロック サイズ（バイト単位）。
[ユニット（Units）] フィールド	ユニット数。

c) [次へ（Next）] をクリックします。

ステップ 13 [電源グループ認定（Power Group Qualifications）] ページで、次の手順を実行して電源グループ認定をポリシーに追加するか、それらを追加しない場合は [次へ（Next）] をクリックします。

a) [電源グループ認定の追加（Add Power Group Qualifications）] チェックボックスをオンにします。

b) [電源グループ（Power Group）] ドロップダウン リストから、ポリシーに含める電源グループを選択します。

c) [次へ（Next）] をクリックします。

ステップ 14 [ラック認定（Rack Qualifications）] ページで、次の手順を実行してラックマウント サーバ認定をポリシーに追加するか、それらを追加しない場合は [次へ（Next）] をクリックします。

a) [ラック認定の追加（Add Rack Qualifications）] チェックボックスをオンにします。

b) [最初のスロットID（First Slot ID）] フィールドに、このポリシーに関連付けられているサーバ プールが取得できる最初のラックマウント サーバ ID を入力します。
アダプタの条件を保存すると、このタイプは変更できなくなります。

c) [スロット数（Number of Slots）] フィールドに、プールに含めるラックマウント サーバ スロットの合計数を入力します。この場合、[最初のスロットID（First Slot ID）] フィールドで指定したサーバ スロットから数え始めます。

d) [次へ（Next）] をクリックします。

ステップ 15 [サーバモデル認定（Server Model Qualifications）] ページで、次の手順を実行してラックマウント サーバ認定をポリシーに追加するか、それらを追加しない場合は [次へ（Next）] をクリックします。

a) [サーバモデル認定の追加（Add Server Model Qualifications）] チェックボックスをオンにします。

b) [モデル(正規表現)（Model(RegEx)）] フィールドに、サーバ モデル PID が一致する必要がある正規表現を入力します。

c) [次へ（Next）] をクリックします。

ステップ 16 [送信（Submit）] をクリックします。

サーバ プール ポリシーの概要

このポリシーはサーバ ディスカバリ プロセス中に呼び出されます。これは、サーバ プール ポリシー資格情報により、サーバと、ポリシーで指定されたターゲット プールが一致した場合にどのような処理が行われるかを定義します。

サーバが複数のプールに適合したときに、これらのプールにサーバ プール ポリシーがあった場合、このサーバはこれらすべてのプールに追加されます。

サーバ プール ポリシーの作成

はじめる前に

このポリシーでは、次のリソースの 1 つ以上がシステムにすでに存在している必要があります。

- 1 つ以上のサーバ プール。
- サーバ プール ポリシー資格情報（サーバをプールに自動的に追加する場合）。

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 ポリシーを作成する組織をクリックして [詳細の表示（View Details）] をクリックします。

ステップ 5 [サーバ プール ポリシー（Server Pool Policies）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [サーバ プール ポリシーの作成（Create Server Pool Policy）] 画面で、次のフィールドに値を入力します。

名前	説明
[名前（Name）] フィールド	ポリシーの一意の名前。
[説明（Description）] フィールド	ポリシーの説明。

名前	説明
[ターゲットプール（Target Pool）] ドロップダウン リスト	ポリシーに関連付けるサーバプールを選択します。
[認定（Qualification）] ドロップダウン リスト	ポリシーに関連付けるサーバプール資格情報ポリシーを選択します。

ステップ 8 [送信（Submit）] をクリックします。

vNIC/vHBA 配置ポリシー

vNIC/vHBA 配置ポリシーは、次のことを決定するために使用されます。

- 仮想ネットワーク インターフェイス接続（vCon）をサーバ上の物理アダプタにマッピングする方法。
- 各 vCon に割り当てることのできる vNIC または vHBA のタイプ。

各 vNIC/vHBA 配置ポリシーには、物理アダプタの仮想表現である vCon が含まれます。vNIC/vHBA 配置ポリシーがサービス プロファイルに割り当てられ、サービス プロファイルがサーバに関連付けられると、vNIC/vHBA 配置ポリシー内の vCon が物理アダプタに割り当てられ、vNIC および vHBA がそれらの vCon に割り当てられます。

1 つのアダプタを持つブレード サーバやラック サーバの場合は、Cisco UCS がすべての vCon をそのアダプタに割り当てます。4 つのアダプタを持つサーバの場合は、Cisco UCS が vCon1 をアダプタ 1 に、vCon2 をアダプタ 2 に、vCon3 をアダプタ 3 に、vCon4 をアダプタ 4 に割り当てます。

2 つまたは 3 つのアダプタを搭載したブレード サーバまたはラック サーバの場合、Cisco UCS は、サーバのタイプと選択された仮想スロット マッピング スキーム（[ラウンドロビン] または [線形順序]）に基づいて vCon を割り当てます。使用可能なマッピング スキームの詳細については、vCon のアダプタへの配置, （77 ページ）を参照してください。

Cisco UCS は、vCon の割り当て後、vNIC と vHBA を各 vCon の [選択プリファレンス（Selection Preference）] に基づいて割り当てます。これは、次のいずれかになります。

- [すべて（All）]：設定されたすべての vNIC と vHBA は、明示的な割り当て、割り当て解除、動的のいずれかで vCon に割り当てられます。これがデフォルトです。
- [割り当てのみ（Assigned Only）]：vNICs と vHBA を vCon に明示的に割り当てる必要があります。サービス プロファイルや vNIC または vHBA のプロパティにより、明示的に割り当てることができます。

- [動的を除く（Exclude Dynamic）]：動的な vNIC や vHBA を vCon に割り当てることはできません。vCon は静的な vNIC と vHBA に使用可能で、割り当て解除または明示的な割り当てを行います。
- [割り当て解除を除く（Exclude Unassigned）]：割り当て解除された vNIC や vHBA を vCon に割り当てることはできません。vCon は動的な vNIC や vHBA の他、明示的に割り当てられた静的な vNIC や vHBA に使用できます。
- [usNIC を除く（Exclude usNIC）]：Cisco usNIC を vCon に割り当てることはできません。vCon は、設定されているその他のすべての vNIC と vHBA に対しては使用可能です。これらの vNIC と vHBA が明示的に割り当てられているか、割り当て解除されているか、または動的かどうかは関係ありません。

（注） [usNIC を除く（Exclude usNIC）] に設定されている vCon に明示的に割り当てられている SRIOV usNIC は、引き続きその vCon に割り当てられたままになります。

vNIC/vHBA 配置ポリシーをサービス プロファイルに含めない場合、Cisco UCS はデフォルトで、vCon マッピング スキームを [ラウンドロビン]、vNIC/vHBA 選択プリファレンスを [すべて] に設定し、各アダプタの機能と相対的な処理能力に基づいて vNIC と vHBA をアダプタに配布します。

vCon のアダプタへの配置

Cisco UCS は、サービス プロファイル内のすべての vCon をサーバ上の物理アダプタにマッピングします。マッピングの実行方法、およびサーバ内の特定のアダプタへの vCon の割り当て方法は、次の条件によって決まります。

- サーバのタイプ。2 つのアダプタ カードを搭載した N20-B6620-2 および N20-B6625-2 ブレード サーバは、他のサポートされるラック サーバまたはブレード サーバとは異なるマッピング スキームを使用します。
- サーバ内のアダプタの数。
- vNIC/vHBA 配置ポリシー内の仮想スロット マッピング スキームの設定（該当する場合）。

vNIC および vHBA を vCon に割り当てるための vNIC/vHBA 選択環境設定を設定するときは、この配置を検討する必要があります。

（注） vCon のアダプタへの配置は、アダプタの PCIE スロット番号とは関係ありません。vCon の配置のために使用されるアダプタ番号は、アダプタの PCIE スロット番号ではなく、サーバ検出中にそれらに割り当てられる ID です。

N20-B6620-2 および N20-B6625-2 ブレード サーバでの vCon のアダプタへの配置

N20-B6620-2 および N20-B6625-2 ブレード サーバの場合は、2 つのアダプタを左から右に、vCon を右から左に数えます。これらのブレード サーバの 1 台が 1 つのアダプタを持つ場合は、Cisco UCS がすべての vCon をそのアダプタに割り当てます。サーバが 2 つのアダプタを持つ場合は、vCon の割り当ては仮想スロット マッピング スキームに基づいて行われます。

- [ラウンド ロビン（Round Robin）]：Cisco UCS は vCon2 と vCon4 をアダプタ 1 に、vCon1 と vCon3 をアダプタ 2 に割り当てます。これがデフォルトです。
- [線形順序（Linear Ordered）]：Cisco UCS は vCon3 と vCon4 をアダプタ 1 に、vCon1 と vCon2 をアダプタ 2 に割り当てます。

vCon のアダプタへの配置（他のすべてのサポート対象サーバの場合）

N20-B6620-2 および N20-B6625-2 ブレード サーバに加え、Cisco UCS によりサポートされるその他すべてのサーバでは、vCon の割り当ては、サーバに搭載されるアダプタ数と仮想スロット マッピング スキームに応じて異なります。

1 つのアダプタを持つブレード サーバやラック サーバの場合は、Cisco UCS がすべての vCon をそのアダプタに割り当てます。4 つのアダプタを持つサーバの場合は、Cisco UCS が vCon1 をアダプタ 1 に、vCon2 をアダプタ 2 に、vCon3 をアダプタ 3 に、vCon4 をアダプタ 4 に割り当てます。

2 つまたは 3 つのアダプタを搭載したブレード サーバまたはラック サーバの場合、Cisco UCS は、選択した仮想スロット マッピング スキーム（[ラウンドロビン] または [線形順序]）に基づいて vCons を割り当てます。

表 *1*：ラウンドロビン マッピング スキームを使用した *vCon* のアダプタへの配置

アダプタの数	vCon1 の割り当て	vCon2 の割り当て	vCon3 の割り当て	vCon4 の割り当て
1	アダプタ1	アダプタ1	アダプタ1	アダプタ1
2	アダプタ1	アダプタ2	アダプタ1	アダプタ2
3	アダプタ1	アダプタ2	アダプタ3	アダプタ2
4	アダプタ1	アダプタ2	アダプタ3	アダプタ4

[ラウンドロビン（Round Robin）] はデフォルトのマッピング スキームです。

表 *2*：線形順序マッピング スキームを使用した *vCon* のアダプタへの配置

アダプタの数	vCon1 の割り当て	vCon2 の割り当て	vCon3 の割り当て	vCon4 の割り当て
1	アダプタ1	アダプタ1	アダプタ1	アダプタ1

アダプタの数	vCon1 の割り当て	vCon2 の割り当て	vCon3 の割り当て	vCon4 の割り当て
2	アダプタ1	アダプタ1	アダプタ2	アダプタ2
3	アダプタ1	アダプタ2	アダプタ3	アダプタ3
4	アダプタ1	アダプタ2	アダプタ3	アダプタ4

（注） Cisco UCS B440 M2 ブレード サーバに搭載された 2 つのアダプタで vCon ポリシーを使用している場合は、次のマッピングに注意してください。

- 最初に vCon 2 からアダプタ 1 へのマッピング
- 2 番目に vCon 1 からアダプタ 2 へのマッピング

vNIC/vHBA の vCon への割り当て

Cisco UCS には、vNIC/vHBA 配置ポリシーを使用して vNIC および vHBA を vCon に割り当てるオプションが 2 つあります。つまり、明示的割り当てと暗黙的割り当てです。

vNIC および vHBA の明示的割り当て

明示的割り当てでは、vCon を指定してから、vNIC または vHBA を割り当てるアダプタを指定します。この割り当てオプションは、サーバ上のアダプタ間への vNIC および vHBA の配布方法を決定する必要がある場合に使用します。

明示的割り当ての場合に、vCon と関連付けられる vNIC および vHBA を設定するには、次の手順を実行します。

- vCon 設定を任意の使用可能なオプションに設定します。vCon は、vNIC/vHBA 配置ポリシーを使用して設定するか、サーバに関連付けられているサービス プロファイルで設定できます。vCon で [すべて（All）] が設定されている場合でも、vNIC または vHBA をその vCon に明示的に割り当てることができます。
- vNIC および vHBA を vCon に割り当てます。この割り当ては、vNIC または vHBA の仮想ホストインターフェイス配置プロパティを使用して行うか、またはサーバに関連付けられているサービス プロファイルで設定できます

vNIC または vHBA を、当該タイプの vNIC または vHBA 用に設定されていない vCon に割り当てようとすると、設定エラーを示すメッセージが表示されます。

サービス プロファイルの関連付け中に、Cisco UCS は、設定済みの vNIC および vHBA の割り当てを、サーバ内の物理的なアダプタ数および機能と比較して検証し、その後でポリシー内の設定

に従って vNIC および vHBA を割り当てます。負荷分散は、このポリシー内で設定された vCon およびアダプタへの明示的な割り当てを元にして実行されます。

1 つ以上の vNIC または vHBA の割り当てがアダプタでサポートされない場合、Cisco UCS は、サービス プロファイルに対する障害を発生させます。

vNIC および vHBA の暗黙的割り当て

暗黙的割り当てでは、Cisco UCS は vCon を決定した後で、アダプタの機能とそれらの相対的な処理能力に基づいて vNIC または vHBA を割り当てるアダプタを決定します。この割り当てオプションは、vNIC または vHBA が割り当てられるアダプタがシステム設定で重要ではない場合に使用します。

暗黙的割り当ての場合に vCon を設定するには、次の手順を実行します。

- vCon 設定を [すべて（All）]、[動的を除く（Exclude Dynamic）]、または [未割り当てを除く（Exclude Unassigned）] に設定します。vCon は、vNIC/vHBA 配置ポリシーを使用して設定するか、サーバに関連付けられているサービス プロファイルで設定できます。
- vCon 設定を [割当済みのみ（Assigned Only）] にしないでください。この設定を使用して暗黙的割り当てを実行することはできません。
- vNIC または vHBA を vCon に割り当てないでください。

サービス プロファイルの関連付け中に、Cisco UCS は、サーバ内の物理的なアダプタ数および機能を検証し、必要に応じて vNIC および vHBA を割り当てます。負荷分散はアダプタの機能に基づいて実行され、vNIC および vHBA の配置は、システムで決定された実際の順序に従って実行されます。たとえば、1 つのアダプタが他のアダプタより多くの vNIC を処理できる場合、そのアダプタにより多くの vNIC が割り当てられます。

サーバに設定されている数の vNIC および vHBA をアダプタでサポートできない場合、Cisco UCS は、サービス プロファイルに対する障害を発生させます。

デュアル アダプタ環境での vNIC の暗黙的割り当て

各スロットにアダプタ カードが搭載されたデュアル スロット サーバで暗黙的な vNIC 割り当てを使用する場合、Cisco UCS は通常 vNIC/vHBA を次のように割り当てます。

- サーバの両方のスロットに同じアダプタがある場合、Cisco UCS は、各アダプタに vNIC と vHBA を半分ずつ割り当てます。
- サーバに 1 つの 非 VIC アダプタと 1 つの VIC アダプタがある場合、Cisco UCS は、2 つの vNIC と 2 つの vHBA を非 VIC アダプタに割り当て、残りの vNIC と vHBA を VIC アダプタに割り当てます。
- サーバに 2 つの異なる VIC アダプタがある場合、Cisco UCS は、2 つのアダプタの相対的な処理能力に基づいて、vNIC と vHBA を比例的に割り当てます。

次の例は、サポートされるアダプタ カードのさまざまな組み合わせに対して、Cisco UCS が vNIC と vHBA をどのように割り当てるのか、その一般的な方法を示しています。

- 4 つ の vNIC と、2 つの Cisco UCS M51KR-B Broadcom BCM57711アダプタ（それぞれ 2 つの vNIC）を搭載したサーバを設定する場合、Cisco UCS は 2 つの vNIC を各アダプタに割り当てます。
- 50 の vNIC と、Cisco UCS CNA M72KR-Eアダプタ（2 つの vNIC）および Cisco UCS M81KR 仮想インターフェイス カードアダプタ（128 の vNIC）を搭載したサーバを設定する場合、Cisco UCS は、2 つの vNIC を Cisco UCS CNA M72KR-Eアダプタに割り当て、48 の vNIC を Cisco UCS M81KR 仮想インターフェイス カードアダプタに割り当てます。
- 150 の vNIC と、Cisco UCS M81KR 仮想インターフェイス カードアダプタ（128 の vNIC）および Cisco UCS VIC-1240 仮想インターフェイス カードアダプタ（256 の vNIC）を搭載したサーバを設定する場合、Cisco UCS は、50 の vNIC を Cisco UCS M81KR 仮想インターフェイス カードアダプタに割り当て、100 の vNIC を Cisco UCS VIC-1240 仮想インターフェイス カードアダプタに割り当てます。

（注） ファブリック フェールオーバー用の vNIC を設定した場合と、サーバ用に動的 vNIC を設定した場合は、この暗黙的割り当ての例外が発生します。

vNIC ファブリックのフェールオーバーが含まれる設定で、1 つのアダプタが vNIC のフェールオーバーをサポートしない場合、Cisco UCS は、ファブリックのフェールオーバーが有効になっているすべての vNIC を、それらをサポートするアダプタに割り当てます。ファブリックのフェールオーバー用に設定された vNIC のみが設定に含まれる場合、それらをサポートしないアダプタに割り当てられる vNIC はありません。ファブリックのフェールオーバー用に設定された vNIC と設定されていない vNIC がある場合、Cisco UCS は、すべてのフェールオーバー vNIC を、それらをサポートするアダプタに割り当て、上記の比率に従って、少なくとも 1 つの非フェールオーバー vNIC を、それらをサポートしないアダプタに割り当てます。

動的 vNIC が含まれる設定の場合、同じ暗黙的割り当てが実行されます。Cisco UCS は、すべての動的 vNIC を、それらをサポートするアダプタに割り当てます。ただし、動的 vNIC と静的 vNIC の組み合わせを使用する場合は、少なくとも 1 つの静的 vNIC が動的 vNIC をサポートしないアダプタに割り当てられます。

vNIC/vHBA 配置ポリシーの作成

手順

ステップ 1 [物理（Physical）] > [コンピューティング（Compute）] の順に選択します。

ステップ 2 [コンピューティング（Compute）] ページで、Cisco UCS Manager アカウントを含むポッドを選択します。

ステップ 3 [組織（Organizations）] をクリックします。

ステップ 4 ポリシーを作成する組織をクリックして [詳細の表示（View Details）] をクリックします。

ステップ 5 [vNic または vHba 配置ポリシー（vNIC/vHBA Placement Policies）] をクリックします。

ステップ 6 [追加（Add）] をクリックします。

ステップ 7 [ネットワーク制御ポリシーの追加（Add Network Control Policy）] 画面で、次のフィールドに入力します。

名前	説明
[名前（Name）] フィールド	ポリシーの一意の名前。

名前	説明
[仮想スロット（Virtual Slot）] ドロップダウン リスト	各仮想スロットの仮想ネットワーク インターフェイスを選択します。次のいずれかになります。 • [すべて（All）]：設定されたすべての vNIC と vHBA は、明示的な割り当て、割り当て解除、動的のいずれかで vCon に割り当てられます。これがデフォルトです。 • [割り当てのみ（Assigned Only）]：vNICs と vHBA を vCon に明示的に割り当てる必要があります。サービス プロファイルや vNIC または vHBA のプロパティにより、明示的に割り当てることができます。 • [動的を除く（Exclude Dynamic）]：動的な vNIC や vHBA を vCon に割り当てることはできません。vCon は静的な vNIC と vHBA に使用可能で、割り当て解除または明示的な割り当てを行います。 • [割り当て解除を除く（Exclude Unassigned）]：割り当て解除された vNIC や vHBA を vCon に割り当てることはできません。vCon は動的な vNIC や vHBA の他、明示的に割り当てられた静的な vNIC や vHBA に使用できます。 • [usNIC を除く（Exclude usNIC）]：Cisco usNIC を vCon に割り当てることはできません。vCon は、設定されているその他のすべての vNIC と vHBA に対しては使用可能です。これらの vNIC と vHBA が明示的に割り当てられているか、割り当て解除されているか、または動的かどうかは関係ありません。 （注） [usNIC を除く（Exclude usNIC）] に設定されている vCon に明示的に割り当てられている SRIOV usNIC は、引き続きその vCon に割り当てられたままになります。

ステップ 8 [送信（Submit）] をクリックします。

配置ポリシー

配置ポリシーは、vCon を選択して vNIC および vHBA にマッピングできる Cisco UCS Director ポリシーです。選択する設定に応じて、システムで配置を自動的に実行するか、自分で配置を選択するか、vNIC/vHBA 配置ポリシーを使用して配置を決定することができます。

このポリシーは、vNIC または vHBA をサーバ上の物理アダプタに割り当てます。各配置ポリシーには、物理アダプタの仮想表現である vCon（仮想ネットワーク インターフェイス接続）が含まれます。vNIC/vHBA 配置ポリシーがサービス プロファイルに割り当てられ、サービス プロファイルがサーバに関連付けられると、配置ポリシー内の vCon が物理アダプタに割り当てられます。アダプタが 1 つだけのサーバの場合、両方の vCon がアダプタに割り当てられます。アダプタが 2 つのサーバの場合、1 つの vCon が各アダプタに割り当てられます。

このポリシーはサービスプロファイルに組み込む必要があります。また、このサービスプロファイルを有効にするには、サーバに関連付ける必要があります。

配置ポリシーの作成

はじめる前に

配置ポリシーを作成する前に、『Cisco UCS Manager configuration guides』に記載されている vNIC/vHBA 配置ポリシーのガイドラインを確認し、選択によってどのような影響があるかを理解しておいてください。

手順

ステップ 1 [ポリシー（Policies）] > [物理インフラストラクチャ ポリシー（Physical Infrastructure Policies）] > [UCS Manager] の順に選択します。

ステップ 2 [配置ポリシー（Placement Policy）] をクリックします。

ステップ 3 [追加（Add）] をクリックします。

ステップ 4 [配置ポリシーの追加（Add Placement Policy）] 画面で、次のフィールドに入力します。

a) [ポリシー名（Policy Name）] フィールドに、ポリシーの一意の名前を入力します。

b) [ポリシーの説明（Policy Description）] フィールドに、このポリシーの説明を入力します。

c) [UCSアカウント名（UCS Account Name）] ドロップダウン リストから、このポリシーを追加する Cisco UCS Manager アカウントを選択します。

d) [UCS Organizationの名前（UCS Organization Name）] ドロップダウン リストから、このポリシーを追加する Cisco UCS 組織を選択します。

e) [ストレージポリシー（Storage Policy）] ドロップダウン リストから、このポリシーに適用するストレージ ポリシーを選択します。

f) [ネットワークポリシー（Network Policy）] ドロップダウン リストから、このポリシーに適用するネットワーク ポリシーを選択します。

g) [配置タイプの選択（Select Placement Type）] ドロップダウン リストから、次のいずれかのオプションを選択します。

- [システムによる配置実行（Let System Perform Placement）]：Cisco UCS Director が、vNIC と vHBA の最適な配置を決定します。このオプションを選択した場合は、ステップ 6 に進みます。
- [手動配置（Manual Placement）]：各 vCon の仮想ネットワーク インターフェイス プリファレンスを手動で選択します。このオプションを選択した場合は、ステップ 5 に進みます。
- [配置ポリシーの選択（Select Placement Policy）]：選択した vNIC と vHBA の配置ポリシーが、vNIC と vHBA の配置を決定します。このオプションを選択した場合は、[vNIC/vHBA 配置ポリシーの選択（Select vNIC/vHBA Placement Policy）] ドロップダウン リストからポリシーを選択し、ステップ 6 に進みます。

ステップ 5 手動配置オプションを選択した場合は、次の手順を実行します。

a) [仮想ネットワークインターフェイスの選択の基本設定（Virtual Network Interface Selection Preference）] 領域で、各 vCon のドロップダウン リストから次のオプションのいずれかを選択します。

- [すべて（All）]：設定されたすべての vNIC と vHBA は、明示的な割り当て、割り当て解除、動的のいずれかで vCon に割り当てられます。これがデフォルトです。
- [割り当てのみ（Assigned Only）]：vNICs と vHBA を vCon に明示的に割り当てる必要があります。サービス プロファイルや vNIC または vHBA のプロパティにより、明示的に割り当てることができます。
- [動的を除く（Exclude Dynamic）]：動的な vNIC や vHBA を vCon に割り当てることはできません。vCon は静的な vNIC と vHBA に使用可能で、割り当て解除または明示的な割り当てを行います。
- [割り当て解除を除く（Exclude Unassigned）]：割り当て解除された vNIC や vHBA を vCon に割り当てることはできません。vCon は動的な vNIC や vHBA の他、明示的に割り当てられた静的な vNIC や vHBA に使用できます。
- [usNIC を除く（Exclude usNIC）]：Cisco usNIC を vCon に割り当てることはできません。vCon は、設定されているその他のすべての vNIC と vHBA に対しては使用可能です。これらの vNIC と vHBA が明示的に割り当てられているか、割り当て解除されているか、または動的かどうかは関係ありません。

  （注） [usNIC を除く（Exclude usNIC）] に設定されている vCon に明示的に割り当てられている SRIOV usNIC は、引き続きその vCon に割り当てられたままになります。

b) [次へ（Next）] をクリックします。

c) [仮想インターフェイスの選択（vNIC/vHBA）（Select Virtual Interface (vNIC/vHBA)）] ドロップダウン リストから、vNIC または vHBA を選択します。

d) [追加（Add）] をクリックします。
e) [仮想ネットワークインターフェイスへの割り当て（Assign to Virtual Network Interface）] ドロップダウン リストから、vNIC または vHBA を配置する vCon を選択します。
f) 5c ～ 5e のステップを繰り返して、すべての vNIC と vHBA を配置します。
g) [次へ（Next）] をクリックして、ステップ 6 を実行します。

ステップ 6 [仮想インターフェイスの順序（Virtual Interface Order）] 画面で、次の手順を実行します。

a) [仮想ネットワークインターフェイス（Virtual Network Interface）] 表で、vHBA と vNIC の順序を確認します。
b) 必要に応じて、vNIC または vHBA のチェックボックスをオンにして、次のオプションの 1 つ以上を選択し、インターフェイスの順序を設定します。

- [上に移動（Move UP）] または [下に移動（Move DOWN）] ボタンをクリックし、vNIC と vHBA の順序を移動します。
- [仮想インターフェイスの順序（Virtual Interface Order）] ドロップダウン リストから数値を選択し、順序を設定します。

ステップ 7 配置の設定が完了したら、[送信（Submit）] をクリックします。