



Cisco Intersight 管理モード移行ツールの作業

- [変換のための IMM 移行の追加 \(1 ページ\)](#)
- [クローニングのための IMM 移行の追加, on page 5](#)
- [移行管理, on page 7](#)
- [デバイス管理, on page 8](#)
- [移行準備レポートの説明 \(9 ページ\)](#)
- [UCS Manager/Central 構成の変換 \(11 ページ\)](#)

変換のための IMM 移行の追加

[UCSM/Central から Intersight のサーバープロファイルへのサービスプロファイルの変換 (Converting Service Profiles from UCSM/Central to Server Profiles in Intersight)]

IMM の移行を開始するには、次の手順を実行します。

始める前に

現在実行中および後続のすべての移行に適用される移行のデフォルト設定を設定できます。移行の追加 プロセス中にデフォルト設定を変更することもできます。詳細については、「[付録 C: 移行設定](#)」の「[変換のデフォルト移行設定](#)」セクションを参照してください。

- ステップ 1 [IMM 移行の追加 (Add IMM Transition)] をクリックします。
- ステップ 2 移行の名前を入力します。
- ステップ 3 移行のタイプを選択します。

(a) UCS Manager ハードウェアおよび構成の互換性/readiness 概要のみを表示する場合、または UCS Central 構成の互換性のみを表示する場合は、[[Readiness レポートの生成 \(Generate Readiness Report\)](#)]

(b) 準備レポートを表示し、変換された構成を Intersight にプッシュする場合は、[[準備レポートの生成 \(Generate Readiness Report\)](#)] + [[構成を Intersight にプッシュ \(Push Config to Intersight\)](#)] を選択します。

(c) 構成をクローニングして、ある Intersight アカウントから別のアカウントに移行する場合は、**[Intersight のクローニング (Clone Intersight)]** を選択します。詳細な手順については、「[クローニングのための IMM 移行の追加](#)」を参照してください。

ステップ 4 [次へ (Next)] をクリックします。

ステップ 5 必要に応じて、プロキシ設定を有効にします。プロキシ設定を有効にする手順については、「[付録 D : プロキシ設定](#)」を参照してください。

ステップ 6 ソース デバイス (UCS Manager または UCS Central) を選択します。

ステップ 7 選択したデバイスの詳細を入力します。

(a) 既存のデバイスの構成を移行する場合は、**[既存の UCS Manager の選択/既存の UCS Central の選択 (Select Existing UCS Manager/ Select Existing UCS Central)]** オプションを選択します。

(b) 新しい UCS Manager/UCS Central 構成を追加する場合は、**[新しい UCS Manager の追加/新しい UCS Central の追加 (Add New UCS Manager/ Add New UCS Central)]** オプションを選択します。該当のデバイスのデバイス IP / FQDN、ユーザー名とパスワードを入力します。

ステップ 8 **[更新 (Refresh)]** をクリックして、UCS Manager/Central デバイスから最新の構成とインベントリの詳細を取得します。

選択したソース デバイスが UCS Central の場合、**[UCS Central の選択 (Choose UCS Central)]** ドロップダウンリストから UCS Central インスタンスを選択できます。

[ダウンロード (Download)] リンクを使用して、現在のデバイスの構成 JSON ファイルとインベントリ JSON ファイルをダウンロードできます。

構成 JSON ファイルには、既存の UCS Manager/UCS Central ドメインに存在するソフトウェア構成の詳細情報が含まれています。

インベントリ JSON ファイルには、UCS Manager ドメインまたは UCS Central インスタンスのすべての UCS ドメインに存在するハードウェア インベントリの詳細情報が含まれています。

これらのファイルは、トラブルシューティングの目的でテクニカル サポート チームと共有できます。

ステップ 9 [次へ (Next)] をクリックします。

ステップ 10 接続先の Intersight アカウントを選択します。

(a) 既存の Intersight アカウントに構成を移行する場合は、**[既存のアカウントから選択 (Choose from existing account)]** オプションを選択します。手順 13 に進みます。

(b) 新しい **[SaaS Intersight]** または新しい **[Intersight アプライアンス VM (Intersight Appliance VM)]** アカウントに構成を移行する場合は、**[新しいアカウントの追加 (Add new account)]** オプションを選択します。手順 11 に進みます。

(c) 宛先の Intersight アカウントの詳細を追加せずに変換準備レポートを生成する場合は、**[Insight デバイスなしで進む (Proceed without Intersight device)]** オプションを選択します。手順 13 に進みます。

ステップ 11 次の手順を実行して、Intersight から API キー ID を生成します。

1. Intersight アプリケーションにログインします。
2. 右上隅にある歯車アイコンをクリックし、**[設定 (Settings)]** を選択します。

3. [API] セクションで、[API キー (API Keys)] をクリックします。
4. ページの右上にある [API キーの生成] をクリックします。
5. [説明 (Description)] フィールドに名前を入力し、[OpenAPI スキーマバージョン 3 の API キー (API Key for OpenAPI Schema Version 3)] を選択します。

(注) OpenAPI スキーマバージョン 2 は、IMM 移行ツール、リリース 3.0.1 ではサポートされていません。V2 および V3 スキーマの API キーのサポートは、IMM Transition Tool、リリース 3.0.2 以降で利用できます。

6. [生成 (Generate)] をクリックします。

API キー ID と秘密鍵が生成されます。[クリップボードにコピー (Copy to Clipboard)] の青いアイコンを使用して、これらの値をクリップボードにコピーします。IMM 移行ツールアプリケーションに戻ります。

ステップ 12 次のフィールドに入力します。

- API キー ID : 前の手順で生成された API キー ID を入力します。
- 秘密鍵 : Intersight で生成された秘密鍵を入力します。

また、Intersight アプライアンス VM を選択した場合は、FQDN を入力します。

ステップ 13 [次へ (Next)] をクリックします。

ステップ 14 移行に必要な変換オプションを構成します。

- 各移行設定フィールドの詳細については、「[付録 C : 移行設定](#)」を参照してください。
- 作成するすべての新しい移行の既定の構成セットを定義するには、「[付録 C : 移行設定](#)」の「**デフォルト移行設定**」を参照してください。

ステップ 15 [次へ (Next)] をクリックします。

ステップ 16 変換する必要があるサービス プロファイル/テンプレートを選択します。

プロファイル名の横に、物理サーバとの関連付けの詳細が表示されます。サービス プロファイル名にマウスポインタを合わせると、サービス プロファイルまたはテンプレートの説明が表示されます。

上部にある検索バーを使用して、特定のサービス プロファイル/テンプレートを検索できます。

フィルタを適用して、検索バーの横にある [表示 (Show)] ドロップダウンリストに、サービス プロファイルテンプレートのみ、またはサービス プロファイルとテンプレートの両方を表示することができます。

ステップ 17 [次へ (Next)] をクリックします。

ステップ 18 選択した送信元組織をマップされた接続先 Intersight 組織に変換する場合は、[高度な組織マッピング (Advanced Organization Mapping)] をオンのままにします。宛先 Intersight 組織の名前を手動で入力するには、トグル ボタンをオフにし、ルート組織名を入力して、ステップ 20 に進みます。[ソース組織パスを Intersight 組織名に保持 (Keep source Org path in Intersight Org name)] オプションを有効にすることで、宛先 Intersight 組織でソース UCS 組織名を保持することもできます。

- このオプションにより、UCSM から Intersight への変換されたオブジェクトのマッピングを柔軟に制御できます。同じ名前前のマッピング動作とは異なり、カスタマイズされたマッピングでは、アカウントに対して複数の Intersight 組織を作成する必要がありません。[高度な組織マッピング (Advanced Organization Mapping)] オプションは、単一または複数の UCS 組織を Intersight 組織にマップするのに役立ちます。
- [新規追加 (Add New)] オプションを使用して、新しい接続先 Intersight 組織を追加することもできます。

ステップ 19 送信元 UCS 組織、接続先 Intersight 組織を選択し、[今すぐマップ (Map Now)] をクリックします。送信元組織と接続先組織がマッピングされます。マップされると、接続先の Intersight 組織名の横に「マップ済み」タグが表示されます。また、[高度な組織マッピング (Advanced Organization Mapping)] ページの下部にあるマッピング セクションで、マッピングされた送信元組織を表示することもできます。

[すべてマッピング解除 (Un-Map All)] オプションを使用して、選択した Intersight アカウント内の既存の送信元組織から接続先組織へのマッピングをすべて解除します。また、マッピング セクションに移動し、マッピングされたエンティティを選択し、そのエンティティの 3 つのドットをクリックして、マッピング解除オプションを選択することにより、マッピングされた単一のエンティティをマッピング解除できます。

ステップ 20 [次へ (Next)] をクリックします。

[次へ (Next)] は、すべての送信元 UCS 組織が選択され、それぞれの接続先 Intersight 組織にマップされている場合にのみ有効と表示されます。

準備レポートが生成されます。設定属性が UCS Manager/UCS Central から取得され、IMM に変換され、結果のレポートが生成されるため、このプロセスには数分かかる場合があります。

(注) UCS Manager/Central 構成のサイズと接続されているサーバの数によっては、一部の操作が完了するまでにかなりの時間がかかる場合があります (1 時間以上)。

ステップ 21 [レポート (View Report)] をクリックしレポートを表示するか、[ダウンロード (Download)] オプションを使用して PDF 形式でレポートをダウンロードします。

選択した構成のレポート生成は 1 回限りのアクティビティであり、再生成することはできません。これにより、移行の履歴が維持され、いつでも参照できるようになります。構成を編集してレポートを生成する場合は、移行を複製できます。詳細については、「[移行管理](#)」を参照してください。

ステップ 22 [次へ (Next)] をクリックします。

[Intersight へのプッシュ (Push to Intersight)] ページが表示されます。

(注) IMM 移行ツール リリース 1.0.2 以降では、使用可能な構成ファイルをダウンロードして手動で編集し、[詳細オプション] を使用して同じものをアップロードできます。

ステップ 23 [詳細オプション] をクリックし、編集したファイルを参照して、[アップロード] をクリックします。アップロードされたファイルは、構成を Intersight にプッシュするために使用されます。

ステップ 24 [次へ (Next)] をクリックします。

Intersight との接続が確立され、変換された構成属性が Intersight にプッシュされます。

- (注)
- 遷移が Intersight デバイスを使用する Intersight にプッシュされている場合、または UCS Manager/UCS Central デバイスから UCSM 構成/インベントリをフェッチしている場合、デバイスの前のタスクが完了するまで、同じデバイスを他の遷移で使用することはできません。
 - 変換されたポリシーが Intersight にプッシュされている場合は、それらのポリシーのデフォルトパスワードをリセットします。

ステップ 25 [プッシュサマリを表示 (View Push Summary)] をクリックして、変換された各オブジェクトのプッシュステータスを表示します。

この概要により、各オブジェクトのプッシュステータスを知ることができます。各オブジェクトステータスの横にある 3 つのドット (...) をクリックすると、オブジェクトを Intersight にプッシュするために IMM 移行ツールによって実行された詳細なコミットが表示されます。ステータスには、次のいずれかを指定できます。

- 成功 (Success) : 変換されたオブジェクトは、Intersight に正常にプッシュされました。
- スキップ (Skipped) : 変換されたオブジェクトは接続先の Intersight アカウントに既に存在し、プッシュ操作でスキップされました。
- 失敗 (Failed) : 変換されたオブジェクトを Intersight にプッシュできませんでした。

オブジェクトステータスの横にある 3 つのドットをクリックして、プッシュの失敗の理由を確認します。

クローニングのための IMM 移行の追加

Intersight でのアカウントのクローニング

Intersight アカウントのクローニングを開始するには、次の手順を実行します。

ステップ 1 [IMM 移行の追加 (Add IMM Transition)] をクリックします。

ステップ 2 移行の名前を入力します。

ステップ 3 移行のタイプを選択します。

構成をクローニングして、ある Intersight アカウントから別のアカウントに移行する場合は、**[Intersight のクローニング (Clone Intersight)]** を選択します。このオプションは、2 つの SaaS Intersight アカウント間、2 つの仮想アプライアンスアカウント間で、仮想アプライアンス Intersight アカウントからクラウド Intersight アカウントに、またはその逆に構成ポリシーを移行するために使用できます。クローニングでサポートされる機能の詳細については、「[付録 B: クローニングでサポートされる機能](#)」を参照してください。

ステップ 4 [次へ (Next)] をクリックします。

- ステップ 5** 必要に応じて、プロキシ設定を有効にします。プロキシ設定を有効にする手順については、「付録 D : プロキシ設定」を参照してください。
- ステップ 6** 送信元 Intersight アカウントを選択します。
- (a) 既存の Intersight アカウントの構成を移行する場合は、**[既存のアカウントから選択 (Choose from existing account)]** オプションを選択します。
 - (b) 新しい **[SaaS Intersight]** または新しい **[Intersight アプライアンス VM (Intersight Appliance VM)]** アカウントの構成を移行する場合は、**[新しいアカウントの追加 (Add new account)]** オプションを選択します。API キー ID と秘密鍵の詳細については、手順 8 と 9 を参照してください。
- ステップ 7** 接続先の Intersight アカウントを選択します。
- (a) 既存の Intersight アカウントの構成を移行する場合は、**[既存のアカウントから選択 (Choose from existing account)]** オプションを選択し、手順 8 に進みます。
 - (b) 新しい **[SaaS Intersight]** または新しい **[Intersight アプライアンス VM (Intersight Appliance VM)]** アカウントの構成を移行する場合は、**[新しいアカウントの追加 (Add new account)]** オプションを選択し、手順 9 に進みます。
- ステップ 8** **[更新 (Refresh)]** をクリックして、既存の Intersight アカウントから最新の構成を取得し、手順 11 に進みます。
- [ダウンロード (Download)]** リンクを使用して、構成 JSON ファイルをダウンロードできます。
- 構成 JSON ファイルには、既存の Intersight アカウントに存在するソフトウェア構成の詳細情報が含まれています。
- このファイルは、トラブルシューティングの目的でテクニカル サポート チームと共有できます。
- ステップ 9** 次の手順を実行して、Intersight から API キー ID を生成します。
- a. Intersight アプリケーションにログインします。
 - b. 右上隅にある歯車アイコンをクリックし、**[設定 (Settings)]** を選択します。
 - c. **[API]** セクションで、**[API キー (API Keys)]** をクリックします。
 - d. ページの右上にある **[API キーの生成]** をクリックします。
 - e. **[説明 (Description)]** フィールドに名前を入力し、**[OpenAPI スキーマバージョン 3 の API キー (API Key for OpenAPI Schema Version 3)]** を選択します。
- Note** OpenAPI スキーマバージョン 2 は、IMM 移行ツールではサポートされていません。
- f. **[生成 (Generate)]** をクリックします。
- API キー ID と秘密鍵が生成されます。**[クリップボードにコピー (Copy to Clipboard)]** の青いアイコンを使用して、これらの値をクリップボードにコピーします。IMM 移行ツールアプリケーションに戻ります。
- ステップ 10** 次のフィールドに入力します。
- API キー ID : 前の手順で生成された API キー ID を入力します。

- 秘密鍵 : Intersight で生成された秘密鍵を入力します。

また、Intersight アプライアンス VM を選択した場合は、FQDN を入力します。

ステップ 11 [次へ (Next)] をクリックします。

ステップ 12 移行に必要な変換オプションを構成します。

- 各移行設定フィールドの詳細については、「付録C : 移行設定」の「クローニング向けの移行設定」を参照してください。

ステップ 13 [次へ (Next)] をクリックします。

[Intersight へのプッシュ (Push to Intersight)] ページが表示されます。

Note IMM 移行ツール リリース 1.0.2 以降では、使用可能な構成ファイルをダウンロードして手動で編集し、**[詳細オプション]** を使用して同じものをアップロードできます。

ステップ 14 **[詳細オプション]** をクリックし、編集したファイルを参照して、**[アップロード]** をクリックします。アップロードされたファイルは、構成を Intersight にプッシュするために使用されます。

ステップ 15 [次へ (Next)] をクリックします。

Intersight との接続が確立され、変換された構成属性が Intersight にプッシュされます。

ステップ 16 **[プッシュサマリを表示 (View Push Summary)]** をクリックして、変換された各オブジェクトのプッシュステータスを表示します。

この概要により、各オブジェクトのプッシュステータスを知ることができます。各オブジェクトステータスの横にある 3 つのドット (...) をクリックすると、オブジェクトを Intersight にプッシュするために IMM 移行ツールによって実行された詳細なコミットが表示されます。ステータスには、次のいずれかを指定できます。

- 成功 (Success) : 変換されたオブジェクトは、Intersight に正常にプッシュされました。
- スキップ (Skipped) : 変換されたオブジェクトは接続先の Intersight アカウントに既に存在し、プッシュ操作でスキップされました。
- 失敗 (Failed) : 変換されたオブジェクトを Intersight にプッシュできませんでした。

オブジェクトステータスの横にある 3 つのドットをクリックして、プッシュの失敗の理由を確認します。

移行管理

ユーザーによって開始されたすべての遷移は、**[移行 (Transition)]** リスト ページに一覧表示されます。このページには、移行の名前、移行の現在のステータス (キャンセル済み、失敗、未完了、進行中、完了)、タイプ (準備状況レポートの生成、Intersight への移行構成、Intersight のクローン)、最終変更時刻が表示されます。

必要なアクションを実行するには、各遷移レコードにある **[...]** をクリックします。

ステップ1 [レポート (Report)] をクリックして、移行の準備状況レポートを表示します。

このオプションは、キャンセルされた遷移および失敗した遷移では使用できません。

ステップ2 [編集 (Edit)] をクリックして、移行名を変更します。

ステップ3 [削除 (Delete)] をクリックし、移行を削除します。

複数のトランジションを選択し、リストビューの左上にあるゴミ箱ボタンをクリックすると、選択したトランジションをまとめて削除できます。

ステップ4 [クローン (Clone)] をクリックして、既存の移行構成をコピーします。

4(a) 移行の名前を指定します。[未完了 (Incomplete)] のステータスでリスト ページに表示されます。

4(b) [移行名 (Transition)] をクリックして構成を編集し、準備状況レポートを生成して、変更した構成を Intersight にプッシュします。

Note [クローン (Clone)] オプションは、タイプが Intersight のクローンの移行では使用できません。

ステップ5 [ログのダウンロード (Download Logs)] をクリックして、変換ログをファイルにダウンロードします。

デバイス管理

IMM 移行ツール、リリース 1.0.2 以降を使用すると、UCS システムと Intersight デバイスをより適切に管理できます。各デバイスに一意のターゲット IP または FQDN を提供することで、デバイスの重複を避けることができます。

デバイスを追加および管理するには、次の手順を実行します。

ステップ1 [デバイス管理 (Device Management)] に移動します。

ステップ2 [デバイスの追加 (Add Device)] をクリックします。

ステップ3 ドロップダウン リストから [デバイスタイプ (Device Type)] を選択します。

ステップ4 ターゲット IP/FQDN を入力します

ステップ5 ステップ3で選択したデバイスタイプが UCS システムの場合は、デバイスのユーザー名を入力します。そうでない場合は、ステップ7に進みます。

ステップ6 デバイスのパスワードを入力し、ステップ9に進みます。

ステップ7 ステップ3で選択したデバイスタイプが Intersight の場合は、API キーを入力します。

ステップ8 秘密キーを入力します。

ステップ9 [保存 (Save)] をクリックします。

デバイスの詳細は、[デバイス管理] リスト ページに表示されます。

追加されたデバイスは、削除または編集できます。Intersight デバイスで編集できる値は API キーとシークレット キーで、UCS デバイスで編集できる値はユーザー名とパスワードです。



Note 既存のデバイスの削除は、それに関連付けられた遷移がない場合にのみ可能です。

移行準備レポートの説明

IMM 移行準備レポートには、IMM への移行のための UCS Manager または UCS Central デバイスのハードウェアインベントリとソフトウェア構成の互換性の概要が表示されます。

準備レポートは次のセクションに分かれています。

1. **変換スコア**：このセクションには、ハードウェア互換性（UCS Manager ドメインでのみ対応）、ファブリック構成（UCS Manager ドメインでのみ対応）、およびサーバー ポリシー構成のスコア メーターが表示されます。
 - スコアメーターの解釈は、次のように説明できます。
 - 優れています：ほとんどすべてのハードウェア / 構成を Intersight に移行できますが、多少の相違はあります。
 - 非常に良い：ほとんどのハードウェア / 構成は移行できますが、一部のハードウェア / 構成はサポートされていないか、Intersight への移行時に矛盾に直面する可能性があります。
 - 良好：ハードウェア / 構成の約半分は Intersight に移行できますが、残りのハードウェア / 構成はサポートされていないか、Intersight への移行中に矛盾に直面する可能性があります。
 - 悪い：少数のハードウェア / 構成のみを Intersight に移行できますが、多くのハードウェア / 構成がサポートされていないか、Intersight への移行中に矛盾に直面する可能性があります。



(注) 上記の評価は、一般的な使用例に基づいています。特定の環境の詳細レポートを確認して、ドメインへの移行の影響を評価することを強くお勧めします。

2. **全体の要約**：全体の要約セクションは、IMM 変換の注意点、ハードウェア互換性の要約（UCS Manager ドメインでのみ）、および IMM 構成変換の要約で構成されます。

- **Intersight マネージドモード変換の注意点**：このセクションでは、変換プロセスを開始する前に確認する必要がある注意点を示します。変換プロセスに関連するエラーと **Warning**（注意）が表示されます。エラーは変換がサポートされていない要素を示し、**Warning** は完全に変換できない要素のリストを示します。
- **ハードウェア互換性の概要**：ファブリック インターコネクタ、ファブリック エクステンダ、アダプタ、IOモジュール、シャーシ、ブレード、ラックなど、該当するハードウェアコンポーネントごとに個別の円グラフが表示されます。円グラフのカラーコードは、次のように説明されます。
 - 緑色は、ハードウェアが移行に対応していることを示します。
 - オレンジ色は、ハードウェアの互換性のためにファームウェアのアップグレードが必要であることを示しています。
 - 赤色は、ハードウェアが現在移行に対応していないことを示しています。



(注) ハードウェア互換性サマリーは、UCS Central ではなく、UCS Manager ドメインに対してのみ生成および表示されます。

- **Intersight 管理モード構成変換の概要**：このセクションには、UCS Manager と UCS Central オブジェクトと、Intersight の対応する変換されたオブジェクトのマッピングテーブルが表示されます。サーバープロファイルテンプレート、サーバープロファイル、ドメインポリシー、プール、サーバーポリシーなどの論理オブジェクトごとに個別のテーブルが表示されます。

3. **ハードウェアの互換性**：このセクションには、UCS Manager ドメインに関して、インベントリの各コンポーネントの互換性レポートが詳細に表示されます。これは、ファブリックハードウェア互換性レポート、シャーシハードウェア互換性レポート、ラックハードウェア互換性レポートなどで構成されています。各コンポーネントをクリックすると、互換性レポートの表が表示されます。この表は、ハードウェアの詳細をリストし、ハードウェアとファームウェアに互換性があるかどうかを示しています。左側の黄色の見出しは、IMM 対応になるためにファームウェアアップグレードが必要なコンポーネントがほとんどないという **Warning**（注意）を示しています。左側の赤い色の見出しは、IMM 移行と互換性のないコンポーネントがほとんどないというエラーを示しています。左側の青色の見出しは、Informational（情報提供）メッセージを示しています。
4. **構成変換**：このセクションでは、UCS Manager/Central の選択されたサービスプロファイルテンプレートで各論理オブジェクトの詳細な互換性レポートを示します。各オブジェクトの見出しをクリックすると、説明の表が表示されます。これらの表には、変換中に使用される属性名と値、ソース UCS Manager/Central と変換された Intersight オブジェクトのマッピング、デバイスの起動順序などがリストされて

います。黄色のアイコンは、一部のオブジェクトを完全に変換できなかったという Warning（注意）を示します。赤色のアイコンは、サポートされていないオブジェクトがほとんどなく、変換できないというエラーを示しています。青色のアイコンは、Informational（情報提供）メッセージを示します。このメッセージに従って対処できます。

5. **ソース構成リファレンス** — このセクションでは、ソース UCS デバイス プールに存在する構成の詳細を示し、サービス プロファイルと物理サーバーに割り当てられた IP アドレスの詳細を提供します。

UCS Manager/Central 構成の変換

IMM 移行ツールで UCS デバイスを追加し、[次へ (Next)] をクリックすると、ユーティリティがバックエンドで実行され、ハードウェア インベントリと構成を検証して、デバイスが IMM と互換性があるかどうかを確認します。

デバイスに接続し、既存の論理属性を複製します。これらには、プロファイル、ポリシー、プール、およびテンプレートが含まれます。

[Intersight へのプッシュ (Push to Intersight)] タスクが正常に完了すると、Intersight アプリケーションは変換されたオブジェクトを更新時に反映します。

換算の前提

IMM 移行ツールでの変換プロセスの前提条件は次のとおりです。

1. **イーサネット ネットワーク制御ポリシー**：Intersight のイーサネット ネットワーク制御ポリシーは、UCS Manager/Central の 2 つの異なる情報ソースを使用して作成できます。
 - サーバー vNIC：UCS Manager/Central のネットワーク制御ポリシーへのマッピング
 - アプライアンス ポート：UCS Manager のアプライアンス ネットワーク制御ポリシーへのマッピング

UCS Manager/Central のネットワーク制御ポリシーを使用して Intersight のイーサネット ネットワーク制御ポリシーを作成する場合、Intersight のイーサネット ネットワーク制御ポリシーの名前は UCS Manager/Central のネットワーク制御ポリシーと同じになります。

UCS Manager のアプライアンス ネットワーク制御ポリシーを使用して Intersight のイーサネット ネットワーク制御ポリシーを作成しているときに、Intersight のイーサネット ネットワーク制御ポリシーの名前は、UCS Manager のネットワーク制御ポリシーの名前に [_appliance] というサフィックスが付けられます。

2. **イーサネット ネットワーク グループ ポリシー**：UCS Manager/Central には、同等のイーサネット ネットワーク グループ ポリシーはありません。イーサネット ネットワーク グループ ポリシーの詳細は、VLAN グループから取得できます。各 VLAN グループには VLAN の詳細があり、それらの詳細はイーサネット ネットワーク グループ ポリシーの

作成に使用されます。イーサネット ネットワーク グループ ポリシーの名前は、VLAN グループの名前と同じになります。

3. **イーサネット QoS ポリシー** : UCS Manager/Central の QoS ポリシーは、Intersight でイーサネットと FC QoS ポリシーに分割されます。
4. **ファイバチャネル ネットワーク ポリシー** : UCS Manager/Central には同等のファイバチャネル ネットワーク ポリシーはありません。ファイバーチャネル ネットワーク ポリシーの詳細は、サービスプロファイル (Intersight) の作成中に取得できます。ファイバーチャネル ネットワーク ポリシーの名前は、SAN 接続ポリシーと vHBA の名前に由来します。
5. **ファイバチャネル QoS ポリシー** : UCS Manager/Central の QoS ポリシーは、Intersight でイーサネットと FC QoS ポリシーに分割されます。
6. **IMC アクセス ポリシー** : インバンド ネットワーク設定の IPv4 および IPv6 アドレスの異なる IP プールを持つ UCS Manager/Central のサービスプロファイルの IMC アクセスポリシーの作成は、現在サポートされていません。UCS Manager/Central には、同等の IMC アクセスポリシーはありません。IMC ポリシーの詳細は、サービスプロファイルから取得できます。各サービスプロファイルには、インバンドネットワーク、IPv4 および IPv6 プールがあります。この情報を使用して、IMC アクセスポリシーが作成されます。
 - IMC アクセスポリシーの名前は、インバンド ネットワーク VLAN およびインバンド プールの名前を使用して派生します。名前は、最大 64 文字まで指定できます。
 - UCS Manager/Central では、サービスプロファイルで IPv4 プールと IPv6 プールを選択するための個別のオプションがありますが、Intersight では、IMC アクセスポリシーで IP プールを選択するオプションは 1 つだけです。Intersight で IMC アクセスポリシーを作成する前に、UCS Manager/Central の IPv4 および IPv6 プールを単一のプールにマージすることをお勧めします。しかし、これは実装が複雑です。変換中に、2つの異なる IP プールに属するインバンド IPv4 および IPv6 アドレスを持つサービスプロファイルがある場合、IPv4 固有のプールのみが IMC アクセスポリシーの作成に考慮されます。
7. **IPMI オーバー LAN ポリシー** : Intersight の IPMI オーバー LAN ポリシーは、UCS Manager/Central の IPMI アクセスプロファイルにマッピングされます。IPMI アクセスプロファイルの IPMI ユーザー関連情報は、Intersight のローカル ユーザー ポリシーに移動されます。
8. **iSCSI ブート ポリシー** : UCS Manager/Central に相当する iSCSI ブートポリシーはありません。iSCSI ブートポリシーの詳細は、サービスプロファイルから取得できます。各サービスプロファイルには、独自の iSCSI vNIC セクションがあります。iSCSI vNIC の詳細は、サービスプロファイルの iSCSI ブートパラメータセクション内にあります。この情報を使用して、iSCSI ブートポリシーが作成されます。
 - iSCSI ブートポリシーの名前は、サービスプロファイルと iSCSI vNIC の名前を使用して派生します。

- UCS Manager/Central には、iSCSI vNIC ノードおよび個々の iSCSI vNIC の IQN プール/イニシエータ名を提供するオプションがあります。Intersight には、個々の iSCSI vNIC 用のそのようなオプションはありません。Intersight の場合、IQN は LCP レベルにあります (vNIC にはありません)。
 - 通常、UCS Manager/Central には、vNIC 用に 2 つの iSCSI ブートターゲットを作成するオプションがあり、各ターゲットには独自の CHAP 詳細があります。ただし、Intersight には、iSCSI ターゲットの CHAP 詳細を提供するオプションが 1 つしかありません。
 - CHAP 認証では、ポリシーの作成中にデフォルト パスワードが考慮されます。
9. **iSCSI 静的ターゲット ポリシー** : UCS Manager/Central に同等の iSCSI 静的ターゲット ポリシーはありません。iSCSI 静的ターゲット ポリシーの詳細は、サービスプロファイルから取得できます。各サービスプロファイルには、独自の iSCSI ブートパラメータセクションがあります。これらの iSCSI ブートパラメータを使用して、Intersight で iSCSI 静的ターゲット ポリシーが作成されます。単一の iSCSI インターフェイスの場合、優先順位に基づいて複数のターゲットが存在する可能性があります。したがって、iSCSI ターゲット名は、サービスプロファイル名、iSCSI インターフェイス名、および iSCSI ターゲットの優先度の組み合わせとして設計されます。
10. **LAN 接続ポリシー** : UCS Manager/Central では、vNIC を複数の方法で設定できます。
1. **インライン vNIC**
 - スタンドアロン vNIC の使用
 - vNIC テンプレートの使用
 2. **LAN 接続ポリシー**
 - スタンドアロン vNIC の使用
 - vNIC テンプレートの使用
- UCS Manager/Central では、LAN / SAN 接続ポリシー、または vNIC / vHBA テンプレートを使用するかどうかにかかわらず、インライン vNIC / vHBA のいずれかにすることができます。接続を構成する唯一の方法であるため、考えられるすべての組み合わせが考慮され、それに応じて Intersight の LAN / SAN 接続ポリシーに変換されます。
11. **電源ポリシー** : UCS Manager では、グローバルポリシーの電源ポリシーセクションが、Intersight のシャーマンプロファイルで使用され電源ポリシーとして変換されます。
12. **SD カード ポリシー** : UCS Manager/Central に相当する SD カード ポリシーはありません。このポリシーは、UCS Manager/Central のローカルディスク構成ポリシーから情報を読み取ることで作成できます。UCS Manager/Central のローカルディスク構成ポリシーで構成された Flexflash がある場合、同等の SD カード ポリシーが Intersight で作成されます。
13. **[ストレージ ポリシー (Storage Policy)]** :
- ストレージ プロファイルのローカル LUN での自動展開

すべての仮想ドライブは、デフォルトで[自動展開 (Auto Deploy)]です。オプションが[no-auto-deploy]に設定されている場合、サービスプロファイルでマップされたVDとストレージポリシーVDは同じ名前にする必要があります。名前が異なる場合は、無効な構成です。

- UCS Manager/Central の LUN セットは、Intersight のシングル ドライブ RAID 構成に相当します。
 - LUN セット内のすべてのディスク スロットを単一の番号のアレイにマージします。
 - すべてのドライブの VD 構成は同一である必要があります。各 LUN セットに異なる VD 構成がある場合は、無効な構成としてフラグを立てます。
- M.2 ドライブの構成
 - UCS Manager/Central で[未指定 (Unspecified)]に設定されている LUN サイズは、ExpandToAvail フラグが True に設定されている仮想ドライブに対してのみ使用する必要があります。フラグが False に設定されている場合、それは無効な構成です。
 - 特定のストレージプロファイルと汎用ストレージプロファイルを持つ UCS Manager/Central のサービスプロファイルをマージして、Intersight で単一のストレージプロファイルを形成します。

14. [VLAN ポリシー (VLAN Policy)] :

Intersight の VLAN ポリシーは、UCS Manager の VLAN セクションにマップされます。UCS Manager では、VLAN の作成中にファブリック ID (A または B、または両方) を選択するオプションがありますが、Intersight では同じ状態ではありません。変換の一環として、ファブリック ID の値が VLAN ポリシーの名前にサフィックスとしてファブリック ID を付加することによって[A]または[B]に設定されている場合、2つの異なる VLAN ポリシーが作成されます。ファブリック ID 値が[両方 (Both)]に設定されている場合、単一の VLAN ポリシーが作成されます。共有タイプをプライマリ/分離/コミュニティとして選択して、プライベート VLAN を作成することもできます。プライマリ VLAN は必須オプションです。指定しない場合、プライベート VLAN の構成はスキップされます。したがって、デフォルトのマルチキャストポリシーで割り当てられた通常の VLAN に変換します。

15. [VSAN ポリシー (VSAN Policy)] :

Intersight の VSAN ポリシーは、UCS Manager の VSAN セクションにマッピングされます。UCS Manager では、VSAN の作成中にファブリック ID (A または B、または両方) を選択するオプションがありますが、Intersight では同じ状態ではありません。変換の一環として、ファブリック ID の値が VSAN ポリシーの名前にサフィックスとしてファブリック ID を付加することによって[A]または[B]に設定されている場合、2つの異なる VSAN ポリシーが作成されます。ファブリック ID 値が[両方 (Both)]に設定されている場合、単一の VSAN ポリシーが作成されます。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。