



物理インフラストラクチャの管理

この章は、次の項で構成されています。

- 「物理インフラストラクチャの管理について」(P.5-1)
- 「接続のテスト」(P.5-4)
- 「デバイス検出の確認」(P.5-5)



(注) 当該アプライアンスにログインしてからでないと、以下の手順はいずれも実行できません。

物理インフラストラクチャの管理について

Cisco UCS Director では、物理と仮想と両方のインフラストラクチャを管理できます。

Cisco UCS Director は、新たに作成された物理アカウントに含まれるすべてのコンポーネントを検出します。通常、この検出プロセスには 5 分ほどかかります。

データセンターを追加することも、デフォルトのデータセンターを使用することも可能です。物理アカウントは、デフォルトのデータセンターと追加したデータセンターの両方に関連付けられます。





(注) 物理と仮想、どちらのタイプのインフラストラクチャを先に追加しても構いません。Cisco UCS Director の物理アカウントには、仮想（クラウド）アカウントとの依存関係はありません。

データセンターの追加

- ステップ 1** [管理] > [物理アカウント] の順にクリックします。
- ステップ 2** [データセンター] タブを選択します。
- ステップ 3** [追加] (+) をクリックします。

ステップ 4 [データセンターの追加] ダイアログボックスで、以下のフィールドを入力します。

名前	説明
[名前] フィールド	データセンターの内容を表す名前。
[タイプ] ドロップダウンリスト	<p>追加するタイプを選択します。ポッドタイプとは、デバイスのタイプ、ベンダー、モデルに基づいて特定のデバイスを論理的にグループ化したものです。以下のいずれかのポッドタイプを選択できます。</p> <ul style="list-style-type: none"> • [FlexPod] • [GenericPod] • [ExpressPod ミディアム] • [ExpressPod スモール] • [VSPEX] • [Vblock] <p> (注) 一般的には、選択したポッドタイプに属しているデバイスタイプだけを追加できます。例外は [GenericPod] で、これはあらゆるデバイスに対応します。</p> <p> (注) [ExpressPod スモール] または [ExpressPod ミディアム] に互換デバイスを追加する場合は、スモールまたはミディアムのポッドライセンスが必要です。それ以外のすべてのポッドタイプで必要なのはデバイスタイプの互換性だけです。</p>
[説明] フィールド	(オプション) データセンターの説明。
[住所] フィールド	データセンターの物理的な所在地。たとえば、都市名や、データセンターの識別用として内部的に利用されるその他の ID などを入力できます。

ステップ 5 [追加] をクリックします。

物理アカウントの追加

ステップ 1 [管理] > [物理アカウント] の順にクリックします。

ステップ 2 [物理アカウント] タブを選択します。

ステップ 3 [追加] (+) をクリックします。

ステップ 4 [アカウントの追加] ダイアログボックスで、以下のフィールドを入力します。

名前	説明
[データセンター] ドロップダウンリスト	その物理アカウントが所属しているデータセンターを選択します。
[カテゴリ] ドロップダウンリスト	<p>カテゴリタイプ ([コンピューティング] または [ストレージ]) を選択します。</p> <p>[ストレージ] を選択した場合はステップ 5 に進みます。</p>

名前	説明
[アカウントタイプ] ドロップダウン リスト	その物理アカウントのアカウント タイプを選択します。次のいずれかを指定できます。 <ul style="list-style-type: none"> • [UCSM] • [HP ILO] • [Cisco ラックサーバ (CIMC)] • [IPMI]
[認証タイプ] ドロップダウン リスト	そのアカウントに使用する認証タイプを選択します。次のいずれかになります。 <ul style="list-style-type: none"> • [ローカルで認証済み]: ローカルで認証されたユーザ アカウントとは、ファブリック インターコネクタを介して直接認証されたユーザ アカウントのことであり、管理者権限または AAA (認証、認可、アカウントティング) 権限を持っていれば誰でも有効/無効にすることができます。 • [リモートで認証済み]: リモートで認証されたユーザ アカウントとは、LDAP、RADIUS、TACACS+ のいずれかを介して認証されたユーザ アカウントのことです。
[アカウント名] フィールド	追加する物理アカウントに割り当てる一意の名前。
[サーバのアドレス] フィールド	サーバの IP アドレス。
[ユーザ ID] フィールド	そのアカウントにアクセスする際に使用するユーザ名。
[パスワード] フィールド	ユーザ名に関連付けられるパスワード。
[トランスポートタイプ] ドロップダウン リスト	アカウントに使用するトランスポート タイプを選択します。次のいずれかになります。 <ul style="list-style-type: none"> • http • https
[ポート] フィールド	サーバのポート番号。
[説明] フィールド	(オプション) アカウントの説明。
[連絡先の電子メール] フィールド	(オプション) アカウントの連絡先の電子メール アドレス。
[ロケーション] フィールド	(オプション) ロケーション。
[サービスプロバイダー] フィールド	(オプション) サービス プロバイダーの名前 (存在する場合)。

ステップ 5 アカウントが [ストレージ] である場合は、[NetApp ONTAP]、[NetApp OnCommand]、[EMC VNX]、[EMC VMAX ソリューションイネーブラ] の中から適切なアカウント タイプを選択します。

ステップ 6 [追加] をクリックします。

ネットワーク要素の追加

ステップ 1 [管理] > [物理アカウント] の順にクリックします。

ステップ 2 [マネージドネットワーク要素] タブを選択します。

■ 接続のテスト

ステップ 3 [ネットワーク要素の追加] をクリックします。

ステップ 4 [ネットワーク要素の追加] ダイアログボックスで、以下のフィールドを入力します。

名前	説明
[データセンター] ドロップダウン リスト	そのネットワーク要素が所属しているデータセンター。
[デバイスカテゴリ] ドロップダウン リスト	そのネットワーク要素のデバイス カテゴリ。
[デバイス IP] フィールド	デバイスの IP アドレス。
[プロトコル] ドロップダウン リスト	使用するプロトコル。次のいずれかになります。 <ul style="list-style-type: none"> • telnet • ssh
[ポート] フィールド	使用するポート。
[ログイン] フィールド	ログイン名。
[パスワード] フィールド	ログイン名に関連付けられるパスワード。
[パスワードの有効化] フィールド	そのネットワーク要素のイネーブルパスワード。

ステップ 5 [送信] をクリックします。

DHCP ログイングの有効化

ステップ 1 [管理] > [物理アカウント] の順にクリックします。

ステップ 2 [ネットワークサービスエージェント] タブを選択します。

ステップ 3 [組み込みネットワークサービス] をクリックします。

ステップ 4 [組み込みネットワークサービス] ダイアログボックスで、[DHCP ログイングを有効にする] チェックボックスをオンにします。

接続のテスト

ステップ 1 [管理] > [物理アカウント] の順にクリックします。

ステップ 2 [物理アカウント] タブを選択します。

ステップ 3 テストするアカウントを選択します。

ステップ 4 [テスト接続] をクリックします。

デバイス検出の確認

- ステップ 1** [管理] > [物理アカウント] の順にクリックします。
- ステップ 2** デバイスの検出を確認するアカウントをクリックします。
- ステップ 3** [検出されたデバイス] タブを選択します。
- ステップ 4** [設定の検出] をクリックします。
- ステップ 5** [設定の検出] ダイアログボックスで、以下のフィールドを確認します。

名前	説明
[検出を有効化] チェックボックス	このチェックボックスはデフォルトでオンになり、アカウントのデバイス検出が有効化されます。
[IP 範囲]	デバイス検出の対象となる IP アドレスの範囲。
[TCP タイムアウト(ミリ秒単位)]	TCP のタイムアウト (ミリ秒単位)。
[SNMP タイムアウト(ミリ秒単位)]	SNMP のタイムアウト (ミリ秒単位)。
[SNMP コミュニティストリング]	SNMP のコミュニティストリング (デフォルトは public)。

- ステップ 6** [送信] をクリックします。

