



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.6-1)
- 「接続のテスト」(P.6-5)
- 「デバイスの検出の有効化」(P.6-6)



(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、物理および仮想の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。

ポッドを追加することも、デフォルトのポッドを使用することも可能です。物理アカウントは、デフォルトのポッドにも、追加したポッドにも関連付けることができます。



(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。

サイトの追加

- ステップ 1** メニューバーで、[管理]>[物理アカウント]の順に選択します。
- ステップ 2** [サイト管理]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** [サイトの追加]ダイアログボックスで、以下のフィールドに値を入力します。

名前	説明
[サイト名]フィールド	サイトの識別に役立つ名前。
[説明]フィールド	(オプション) サイトの説明（ロケーションや重要性など）。
[連絡名]フィールド	このサイトの担当者の名前。

ステップ 5 [送信] をクリックします。

ポッドの追加

ステップ 1 メニュー バーで、[管理] > [物理アカウント] の順に選択します。

ステップ 2 [ポッド] 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 [ポッド] ダイアログボックスで、以下のフィールドに値を入力します。

名前	説明
[名前] フィールド	ポッドの識別に役立つ名前。
[タイプ] ドロップダウンリスト	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。 <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) ポッドの説明。
[住所] フィールド	ポッドの物理的な場所。たとえば、都市名や、ポッドに使用されるその他の内部的な 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 メニュー バーで、[管理] > [物理アカウント] の順に選択します。

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、以下のフィールドに値を入力します。

名前	説明
[ポッド] ドロップダウンリスト	この物理アカウントが属しているポッドを選択します。
[カテゴリ] ドロップダウンリスト	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。 [ストレージ] を選択した場合はステップ 5 に進みます。
[アカウントタイプ] ドロップダウンリスト	こ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	このアカウントに使用する認証タイプを選択します。次のいずれかを指定できます。 <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 インターコネクト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) 権限を持っていると誰でも有効/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。
[サーバ管理] ドロップダウンリスト	次のいずれかのオプションを選択して、このアカウントがサーバを管理する方法を選択します。 <ul style="list-style-type: none"> • [すべてのサーバ] • [選択済みのサーバ]
[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	こ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	ユーザ名に関連したパスワード。
[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。

マルチドメイン マネージャ アカウントの追加

- ステップ 1** メニュー バーで、[管理] > [物理アカウント] の順に選択します。
- ステップ 2** [マルチドメインマネージャ] 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、以下のフィールドに値を入力します。

名前	説明
[アカウント名] フィールド	このマルチドメイン マネージャ アカウントが属するアカウント名を選択します。
[説明] フィールド	(オプション) アカウントの説明。
[アカウントタイプ] ドロップダウン リスト	このマルチドメイン マネージャ 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"> • [PNSC] : Cisco Prime Network Services Controller アカウント。 • [UCS セントラル] : Cisco UCS セントラル アカウント。
[サーバのアドレス] フィールド	マルチドメイン マネージャ アカウントを管理するサーバの IP アドレスを入力します。
[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	こ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	ユーザ名に関連したパスワード。
[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。デフォルトのポートは 443 です。
[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。

- ステップ 5** [送信] をクリックします。

ネットワーク要素の追加

- ステップ 1** メニュー バーで、[管理]>[物理アカウント]の順に選択します。
- 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。
- 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
[ポッド] ドロップダウン リスト	ネットワーク要素が属しているポッドを選択します。
[デバイスカテゴリ] ドロップダウン リスト	ネットワーク要素のデバイス カテゴリを選択します。
[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を選択します。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 ロギングの有効化

- ステップ 1** メニュー バーで、[管理]>[物理アカウント]の順に選択します。
- 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 ロギングを有効にする] チェックボックスをオンにします。

接続のテスト

マネージド ネットワーク要素および物理アカウントの接続をテストできます。

マネージド ネットワーク要素の接続のテスト

- ステップ 1 メニュー バーで、[管理]>[物理アカウント]の順に選択します。
- 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。
- ステップ 3 接続をテストするポッドを選択します。
- ステップ 4 [テスト接続] をクリックします。

物理アカウントの接続のテスト

- ステップ 1 メニュー バーで、[管理]>[物理アカウント]の順に選択します。
- 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 接続を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。

デバイスの検出の有効化

- ステップ 1 メニュー バーで、[管理]>[物理アカウント]の順に選択します。
- 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] アイコンをクリックします。[設定の検出] ダイアログボックスが最初に表示されます。
- ステップ 5 [検出を有効にする] チェックボックスをオンにして、検出を有効化します。
- ステップ 6 [設定の検出] ダイアログボックスで、IP アドレス範囲のフィールドに値を入力して、以下のフィールドのデフォルト値が環境に適しているかどうかを判断します。

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、この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 タイムアウト (ミリ秒単位) (デフォルト値は 2000 ms)。
[SNMP タイムアウト(ミリ秒単位)]	SNMP タイムアウト (ミリ秒単位) (デフォルト値は 1500 ms)。
[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 7 [送信] をクリックします。