



UCS シャーシポリシーの設定

- [シャーシポリシー \(1 ページ\)](#)
- [IMC アクセスポリシーの作成 \(2 ページ\)](#)
- [SNMP ポリシーの作成 \(3 ページ\)](#)
- [シャーシの電源ポリシーの作成 \(6 ページ\)](#)
- [温度ポリシーの作成 \(9 ページ\)](#)

シャーシポリシー

Cisco Intersight のシャーシポリシーでは、IP プール設定、VLAN 設定、SNMP 認証、SNMP トラップ設定など、シャーシのさまざまなパラメータを構成できます。シャーシポリシーは、任意の数のシャーシプロファイルに割り当てることで、シャーシの構成基準を提供できます。

Chassis Policies テーブル ビューを表示するには、**Service Selector** ドロップダウンリストから [サービスとしてのインフラストラクチャ (**Infrastructure Service**)] を選択します。[構成 (**Configure**) > ポリシー (**Policies**)] の順に選択します。

Cisco Intersight のシャーシポリシー作成ウィザードには、次の 2 つのページがあります。

- **[全般 (General)]** : 組織を選択し、ポリシーの名前を入力できます。オプションで、ポリシーの識別に役立つ短い説明とタグ情報を含められます。タグは **key : value** 形式である必要があります。たとえば、**Org:IT** または **Site:APJ** などです。
- **[ポリシーの詳細 (Policy Details)]** : ポリシーの詳細ページには、UCS シャーシポリシーに適用可能なプロパティがあります。

シャーシポリシーは、既存のポリシーと同様のプロパティで **[ポリシークローン (Policy Clone)]** ウィザードを使用して複製することもできます。ポリシーの複製アクションは、ポリシーリストと詳細ビューの両方で使用できます。詳細については、「[ポリシーの複製](#)」を参照してください。

Cisco Intersight で設定できるシャーシポリシーは次のとおりです。

- **[IMC アクセスポリシー (IMC Access Policy)]** : IP プールとシャーシプロファイルのマッピングによって、ネットワークを構成し、管理できます。このポリシーを使用すると、VLAN を構成し、IP プールを使用して IP アドレスと関連付けることができます。



(注) シャーシ IMC アクセス ポリシーでは、インバンド構成のみがサポートされます。

- **[SNMP ポリシー (SNMP Policy)]** : 管理対象デバイスから SNMP トラップを利用して障害およびアラート情報を送信するための SNMP 設定を設定します。管理対象デバイスすでに構成されている SNMP ユーザーまたは SNMP トラップは削除され、このポリシーで構成するユーザーまたはトラップに置き換えられます。ポリシーにユーザやトラップを追加していない場合、入出力モジュール (IOM) 上の既存のユーザやトラップは削除されません。
- **[電源ポリシー (Power Policy)]** : シャーシの電源使用の管理を有効にします。このポリシーでは、シャーシ電源装置 (PSU) の冗長モードを設定し、シャーシに電力を割り当てることができます。[シャーシの詳細 (Chassis details)] ビューページの **[全般 (General)]** タブのプロパティセクションで、冗長の正常性、冗長モード、入力電源の正常性、および出力電源の正常性を表示できます。Cisco UCS X9508 シャーシの場合、省電力モードと動的電力再割り当てを設定できます。
- **[温度ポリシー (Thermal Policy)]** : シャーシのファン制御モードの値を設定できます。ファン制御モードは、最適なサーバ冷却を維持するためにシャーシファンの速度を制御します。

IMC アクセス ポリシーの作成

IMC アクセスポリシーでは、VLAN ID を提供し、選択した IP プールからの IP アドレスと関連付けることができます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. **[サービス セレクタ (Service Selector)]** ドロップダウン リストから、**[インフラストラクチャ サービス (Infrastructure Service)]** を選択します。
3. **[ポリシーの構成 (Configure > Policies)]** に移動し、**[ポリシーの作成 (Create Policy)]** をクリックします。
4. **[IMC アクセス (IMC Access)]** を選択し、**[スタート (Start)]** をクリックします。
5. **[全般 (General)]** ページで、次のパラメータを設定します。

[プロパティ (Property)]	[基本情報 (Essential Information)]
[組織 (Organization)]	組織を選択します。
[名前 (Name)]	ポリシーの名前を入力します。
[タグ (Tag、オプション)]	key-value 形式でタグを入力します

[プロパティ (Property)]	[基本情報 (Essential Information)]
[説明 (Description、オプション)]	簡単な説明を入力します。

6. [ポリシーの詳細 (Policy Details)] ページで、次のパラメータを設定します。

[プロパティ (Property)]	[基本情報 (Essential Information)]	
[VLAN ID]	入力インバンドネットワークを介したサーバアクセスに使用される VLAN ID を入力します。フィールド値は 4~4093 です。	
IPv4 アドレス設定	このポリシーのネットワークのタイプを決定する場合に選択します。 (注) IPv4 アドレス設定のみ、または IPv4 と IPv6 の両方の設定を選択できます。	
IPv6 アドレス設定	このポリシーのネットワークのタイプを決定する場合に選択します。IPv6 アドレス設定のみ、または IPv4 と IPv6 の両方の設定を選択できます。 重要 IPv6 は UCS-IOM-2408 でのみサポートされます。	
IP プール	IP プールの選択	クリックして、右側のペインで IP プールリストを表示して選択します。

7. [作成 (Create)] をクリックします。

SNMP ポリシーの作成

SNMP ポリシーでは、管理対象デバイスから SNMP トラップを利用して障害およびアラート情報を送信するための SNMP 設定を設定します。このポリシーは、SNMPv1、SNMPv2 (v2c を含む)、SNMPv3 などの SNMP バージョンをサポートします。管理対象デバイスに設定されている既存の SNMP ユーザまたは SNMP トラップは削除され、このポリシーで設定するユーザまたはトラップに置き換えられます。ポリシーにユーザやトラップを追加していない場合、入出力モジュール (IOM) 上の既存のユーザやトラップは削除されます。

SNMP ポリシーを使用すると、SNMP を有効または無効にしたり、アクセスおよびコミュニティストリングを指定したり、データの取得に使用する SNMP ユーザの詳細を指定したりできます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。

2. [サービス セレクタ (Service Selector)] ドロップダウン リストから、[インフラストラクチャ サービス (Infrastructure Service)] を選択します。
3. [ポリシーの構成 (Configure > Policies)] に移動し、[ポリシーの作成 (Create Policy)] をクリックします。
4. [SNTP] を選択して、[スタート (Start)] をクリックします。
5. [全般 (General)] ページで、次のパラメータを設定します。

[プロパティ (Property)]	[基本情報 (Essential Information)]
[組織 (Organization)]	組織を選択します。
[名前 (Name)]	ポリシーの名前を入力します。
[タグ (Tag、オプション)]	key-value 形式でタグを入力します
[説明 (Description、オプション)]	簡単な説明を入力します。

6. [ポリシーの詳細 (Policy Details)] ページで、次のパラメータを設定します。

[プロパティ (Property)]	[基本情報 (Essential Information)]
[SNMP の有効化 (Enable DNS)]	エンドポイントでの SNMP ポリシーの状態を表示します。エンドポイントから指定ホストに SNMP トラップを送信するには、このオプションを有効にします。
[アクセスコミュニティストリング (Access Community String)]	SNMPv1、SNMPv2 コミュニティストリング、または SNMPv3 ユーザ名を入力します。フィールドには 18 文字まで入力できます。 (注) フィールドが空の場合は、SNMPv1 および SNMPv2c ユーザが無効になっていることを示します。
[トラップコミュニティストリング (Trap Community String)]	他のデバイスに SNMP トラップを送信する際に使用する SNMP コミュニティグループの名前を入力します。 (注) このフィールドは、SNMPv2c トラップホストまたは宛先にのみ適用されます。
[SNMP ユーザ (SNMP Users)]	

[プロパティ (Property)]	[基本情報 (Essential Information)]
[名前 (Name)]	SNMPv3 ユーザ名を入力します。このフィールドは 1~31 文字で指定する必要があります。
[セキュリティ レベル (Security Level)]	エージェントとマネージャーの間での通信で使用するセキュリティ メカニズムを選択します。 <ul style="list-style-type: none"> • AuthPriv • AuthNoPriv
[認証タイプ (Auth Type)]	ユーザの認証プロトコルとして [SHA] を選択します (注) [MD5] 認証プロトコルはサポートされていません。
[認証パスワード (Auth Password)]	ユーザの認証パスワードを入力します。
[認証パスワードの確認 (Auth Password Confirmation)]	ユーザの認証パスワードを確認のため入力します。
[プライバシータイプ (Privacy Type)]	ユーザのプライバシープロトコルとして [AES] を選択します。
[プライバシーパスワード (Privacy Password)]	ユーザのプライバシー パスワードを入力します。
[プライバシーパスワードの確認 (Privacy Password Confirmation)]	ユーザのプライバシー パスワードを確認のため入力します。
[SNMP トラップの宛先 (SNMP Trap Destinations)]	
[有効化 (Enable)]	SNMP ポリシーを許可して展開するには、このオプションを有効にします。
[SNMP バージョン (SNMP Version)]	トラップの SNMP バージョンとして [v2] または [v3] を選択します。
[ユーザ (User)]	トラップの SNMP ユーザを選択します。最大 15 のトラップ ユーザを定義できます。 (注) このフィールドは SNMPv3 にのみ適用されます。

[プロパティ (Property)]	[基本情報 (Essential Information)]
[トラップタイプ (Trap Type)]	宛先にトラップが送信されたとき、どのタイプであれば通知を受信するかを選択します: <ul style="list-style-type: none"> • [トラップ (Trap)] • [情報 (Inform)]
[宛先アドレス (Destination Address)]	SNMP トラップ情報の送信先アドレスを指定します。最大 15 のトラップ宛先を定義できます。
[ポート (Port)]	入力のサーバーがトラップの宛先と通信するために使用するポート番号を入力します。値の範囲は 1 ~ 65535 です。デフォルトは 162 です。

7. [作成 (Create)] をクリックします。

シャーシの電源ポリシーの作成

このポリシーは、シャーシの電源冗長性と電源割り当ての設定を有効にします。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。
2. [サービス セレクタ (Service Selector)] ドロップダウン リストから、[インフラストラクチャ サービス (Infrastructure Service)] を選択します。
3. [ポリシーの構成 (Configure > Policies)] に移動し、[ポリシーの作成 (Create Policy)] をクリックします。
4. [電源 (Power)] を選択し、[スタート (Start)] をクリックします。
5. [全般 (General)] ページで、次のパラメータを設定します。

プロパティ (Property)	基本情報 (Essential Information)
[組織 (Organization)]	組織を選択します。
[名前 (Name)]	ポリシーの名前を入力します。
[タグの設定 (Set Tags、オプション)]	key:value 形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。
[説明 (Description、オプション)]	簡単な説明を入力します。

6. [ポリシーの詳細 (Policy Details)] ページで、[UCS シャーシ (UCS Chassis)] タブに移動します。
7. 次のパラメータを設定します。

プロパティ (Property)	基本情報 (Essential Information)
[電源の冗長性 (Power Redundancy)] シャーシ電源の冗長モードを設定します。	
[グリッド (Grid)]	グリッドモードには2つの電源が必要です。一方の電源がダウンすると、もう一方の電源装置がシャーシに電源を供給します。
[非冗長 (Not Redundant)]	Power Manager は、シャーシの電力要件をサポートするために必要な最小数の PSU をオンにします。冗長 PSU は維持されません。
[N+1]	Power Manager は、シャーシの電源要件をサポートするために必要な最小数の PSU と、冗長性のために 1 つの追加 PSU をオンにします。
[N+2]	Power Manager は、シャーシの電源要件と冗長性のための 2 つの追加 PSU をサポートするために必要な最小数の PSU をオンにします。 (注) このモードは、Cisco-UCSX-9508 シャーシでのみサポートされています。

プロパティ (Property)	基本情報 (Essential Information)
Power Saveモード	<p>要求された電力が利用可能な電力よりも少ない場合に、追加の PSU 容量を省電力モードにすることができます。</p> <p>(注) このプロパティは、以下でサポートされています。</p> <ul style="list-style-type: none"> • 最小 Cisco IMC ファームウェアバージョン 4.2(1d) を搭載した Cisco-UCSX-9508 シャーシ。 • 最小 Cisco IMC ファームウェアバージョン 4.3(2a) を搭載した Cisco-UCSB-5108 シャーシ。
動的パワー リバランス	<p>サーバに電力を動的に再割り当てできるようにします。</p> <p>有効にすると、ブレード、ファン、IOM/IFM、XFM などのさまざまなシャーシコンポーネント間で電力が再バランスされます。</p> <p>(注) このプロパティは、以下でサポートされています。</p> <ul style="list-style-type: none"> • 最小 Cisco IMC ファームウェアバージョン 4.2(1d) を搭載した Cisco-UCSX-9508 シャーシ。 • 最小 Cisco IMC ファームウェアバージョン 4.3(2a) を搭載した Cisco-UCSB-5108 シャーシ。

プロパティ (Property)	基本情報 (Essential Information)
拡張電力容量	<p>シャーシの拡張電力容量を設定します。このモードを有効にすると、冗長電源から電力が借りられ、シャーシが利用できる電力が増加します。</p> <p>(注) このプロパティは、最小 Cisco IMC ファームウェアバージョン 4.2(1d) を搭載した Cisco-UCSX-9508 シャーシでのみサポートされます。</p>
[電力割り当て (ワット) (Power Allocation (Watts))]	<p>シャーシが消費できる最大電力を設定できます。</p> <p>この値は、最小システム要件から最大使用可能電力までの範囲で指定できます。</p> <p>電力割り当てが0のポリシーを展開すると、シャーシバジレットのキャップが解除されます。つまり、シャーシは使用可能なすべての電力を消費できます。</p> <p>(注) このプロパティは、以下でサポートされています。</p> <ul style="list-style-type: none"> • 最小 Cisco IMC ファームウェアバージョン 4.2(1d) を搭載した Cisco-UCSX-9508 シャーシ。 • 最小 Cisco IMC ファームウェアバージョン 4.3(2a) を搭載した Cisco-UCSB-5108 シャーシ。

8. [作成 (Create)] をクリックします。

温度ポリシーの作成

このポリシーにより、シャーシファンの速度を制御できます。

1. Cisco ID で Cisco Intersight にログインし、管理者ロールを選択します。

2. [サービス セレクタ (Service Selector)] ドロップダウン リストから、[インフラストラクチャ サービス (Infrastructure Service)] を選択します。
3. [ポリシーの構成 (Configure > Policies)] に移動し、[ポリシーの作成 (Create Policy)] をクリックします。
4. [サーマル (Thermal)] を選択し、[スタート (Start)] をクリックします。
5. [全般 (General)] ページで、次のパラメータを設定します。

プロパティ (Property)	基本情報 (Essential Information)
[組織 (Organization)]	組織を選択します。
[名前 (Name)]	ポリシーの名前を入力します。
[タグの設定 (Set Tags、オプション)]	key:value 形式でタグを入力しますたとえば、Org: IT または Site: APJ などです。
[説明 (Description、オプション)]	簡単な説明を入力します。

6. [ポリシーの詳細 (Policy Details)] ページで、次のパラメータを設定します。

プロパティ (Property)	基本情報 (Essential Information)
[ファン制御モード (Fan Control Mode)]	シャーシのファン速度を制御します。
[バランス (Balanced)]	サーバで多量の熱が発生すると、ファンはその必要に応じてより高速で稼働します。可能な場合、ファンは必要な最低速度に戻ります。
[ロー パワー (Low Power)]	ファンは、[バランス (Balanced)] モードよりもわずかに低い最小速度で動作し、可能な場合は電力消費を抑えます。
[ハイ パワー High Power)]	ファンは電力消費よりパフォーマンスを重視した、より高い速度を動作します。 (注) このモードは、UCS X シリーズ シャーシでのみサポートされません。

プロパティ (Property)	基本情報 (Essential Information)
[最大パワー (Maximum Power)]	<p>ファンは常に最大速度に維持されます。このオプションでは冷却効果は最大になりますが、電力消費も最大になります。</p> <p>(注) このモードは、UCS X シリーズ シャーシでのみサポートされます。</p>
[音響 (Acoustic)]	<p>大きな音響が問題となる環境でのノイズレベルを減らすために、ファン速度を遅くします。</p> <p>(注) このモードは、UCS X シリーズ シャーシでのみサポートされます。</p>

7. [作成 (Create)] をクリックします。

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。