サーバーの管理

この章は、次の内容で構成されています。

サーバのブート順

Cisco IMC を使用して、使用可能なブートデバイスタイプからサーバがブートを試行する順序を設定できます。レガシーブート順の設定では、Cisco IMC によりデバイスタイプの並び替えが許可されますが、デバイスタイプ内のデバイスの並べ替えはできません。高精度ブート順の設定により、デバイスの線形順序付けができます。Web UI または CLI では、ブート順およびブートモードの変更、各デバイスタイプ下への複数のデバイスの追加、ブート順の並び替え、各デバイス タイプのパラメータの設定ができます。

ブート順の設定を変更すると、Cisco IMC は、サーバが次にリブートされるときに、設定されたブート順を BIOS に送信します。新しいブート順を実装するには、設定の変更後にサーバーをリブートします。新しいブート順は以降のリブートで反映されます。設定されたブート順は、設定が Cisco IMC または BIOS 設定で再度変更されるまで保持されます。

（注） 次のいずれかの条件が発生すると、実際のブート順は設定されたブート順と異なります。

- 設定されたブート順を使用してブートしようとしたときに BIOS で問題が発生した。
- ユーザが BIOS で直接、ブート順を変更した。
- BIOS が、ホストによって認識されているがユーザーから設定されていないデバイスを追加した。

重要 Cisco UCS C220 M5 または C480 M5 サーバをリリース 4.1 (1x) にアップグレードする場合は、次の条件に従います。

- 4.0 よりも前のリリースからアップグレードする場合 (4x)
- **[レガシー ブート モード (Legacy Boot Mode)]** が有効になっていて、**[Cisco IMC のブート順序 (Cisco IMC Boot Order)]** が設定されていない場合
- サーバが Cisco HWRAID アダプタから起動している場合

その後、アップグレードする前に次のいずれかを実行する必要があります。

- ここに記載されている XML API スクリプトと UCSCFG ベースのスクリプトを実行します。

  または

- Cisco IMC GUI または CLI インターフェイスを使用して、目的のブート順序を手動で設定します。

（注） ブート順の設定機能を使用して新しいポリシーを作成する場合、BIOS はこの新しいポリシーをシステムのデバイスにマッピングしようとします。実際にマッピングされたデバイス名とポリシー名が [**Actual Boot Order**] 領域に表示されます。BIOS が Cisco IMC の特定のポリシーにデバイスをマッピングできない場合は、実際のデバイス名が [**Actual Boot Order**] 領域に [**NonPolicyTarget**]として示されます。

（注） Cisco IMC 2.0(x) のアップグレード中に、レガシー ブート順は高精度ブート順に移行されます。前のブート順の設定が削除され、バージョン 2.0 にアップグレードする前に設定されたすべてのデバイス タイプが対応する高精度ブート デバイス タイプに変換され、ダミーのデバイスが同じデバイス タイプ用に作成されます。Web UI の **[構成されたブート順序 (Configured Boot Order)]** 領域でこれらのデバイスを確認できます。CLI でこれらのデバイスを確認するには、**show boot-device** コマンドを入力します。この間に、サーバーの実際のブート順が保持され、Web UI と CLI の実際のブート順オプション下で確認できます。

Cisco IMC を 2.0(x) よりも前のバージョンにダウングレードすると、サーバの最後のブート順が保持され、それを [**Actual Boot Order**] 領域で確認できます。次に例を示します。

- 2.0(x) バージョンでレガシー ブート順でサーバを設定した場合、ダウングレードすると、レガシー ブート順の設定が保持されます。
- 2.0(x) で高精度ブート順でサーバーを設定した場合、ダウングレードすると、最後に設定したレガシー ブート順が保持されます。

重要

- 2.0(x) より前のブート順の設定がレガシー ブート順と見なされます。実行中のバージョンが 2.0(x) の場合、Web UI でレガシー ブート順を設定できませんが、CLI および XML API を介して設定できます。CLI で、**set boot-order HDD,PXE** コマンドを使用してこれを設定できます。CLI または XML API を介してレガシー ブート順を設定できますが、Web UI では設定されたこのブート順は表示されません。
- レガシー ブート順の機能と高精度ブート順の機能は相互に排他的です。レガシー ブート順または高精度ブート順のどちらかを設定できます。レガシーブート順を設定すると、設定されたすべての高精度ブートデバイスがディセーブルになります。高精度ブート順を設定すると、レガシー ブート順の設定が消去されます。

高精度ブート順の設定

始める前に

サーバのブート順を設定するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [コンピューティング（Compute）] メニューをクリックします。

ステップ 2 [BIOS] タブで [Configure Boot Order] タブをクリックします。

ステップ 3 **[BIOS プロパティ (BIOS Properties)]** 領域の **[ブート順序の構成 (Configure Boot Order)]** をクリックします。

[ブート順序の構成 (Configure Boot Order)] ダイアログ ボックスが表示されます。

ステップ 4 [Configure Boot Order] ダイアログボックスで、次のプロパティを更新します。

[Basic] タブ

名前	説明
[Device Types] テーブル	サーバのブート オプション。次の 1 つ以上を選択できます。 • **HDD**：ハード ディスク ドライブ • [FDD]：フロッピー ディスク ドライブ • [CDROM]：ブート可能な CD-ROM または DVD • [PXE]：PXE ブート • **EFI**：Extensible Firmware Interface
>>	選択したデバイス タイプを [Boot Order] テーブルに移動します。
<<	選択したデバイス タイプを [Boot Order] テーブルから削除します。
[Boot Order] テーブル	このサーバーがブートできるデバイス タイプが、ブートが試行される順番に表示されます。
Down	選択したデバイス タイプを [ブート順序（Boot Order）] テーブルで高いプライオリティに移動します。
Up	選択したデバイス タイプを [**Boot Order**] テーブルで高いプライオリティに移動します。
変更の保存	このページで加えた変更を保存する場合に、このボタンをクリックします。
[Close] ボタン	変更を保存しないで、または既存の設定を再適用しないで、ダイアログ ボックスを閉じます。

[Advanced] タブ

[ブート デバイスの追加 (Add Boot Device)] ペインに次のリンクのリストが表示されます。

- **ローカル HDD の追加**
- **[Add PXE Boot]**
- **[Add SAN Boot]**
- **[Add iSCSI Boot**

- **[Add USB]**
- **[Add Virtual Media]**
- **[Add PCHStorage]**
- **[Add UEFISHELL]**
- **NVME の追加**
- **ローカル CDD の追加**
- **HTTPブートの追加**

[高度なブート順序構成 (Advanced Boot Order Configuration)] ペインに、追加されたデバイスが表示されます。適切なボタンを選択すると、次のアクションを実行できます。

- **Enable または Disable**
- **修正**
- **[削除（Delete）]**
- **[クローン（Clone）]**
- **再適用**
- **Move Up**
- **Move Down**

ステップ 5 [Save Changes] をクリックします。

サーバに接続しているデバイスによっては、実際のブート順に追加のデバイス タイプが付加される場合があります。

次のタスク

サーバを再起動して、新しいブート順でブートします。

ブート デバイスの管理

始める前に

デバイス タイプをサーバのブート順に追加するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[コンピューティング（Compute）]メニューをクリックします。

ステップ 2 [BIOS] タブで [Configure Boot Order] タブをクリックします。

ステップ 3 [BIOS Properties] 領域の [Configure Boot Order] をクリックします。

ブート順の説明が示されたダイアログボックスが表示されます。

ステップ 4 [Configure Boot Order] ダイアログボックスで、[**Add Boot Device**] テーブルからブート順に追加するデバイスを選択します。

ローカル HDD デバイスを追加するには、[**Add Local HDD**] をクリックし、次のパラメータを更新します。

名前	説明
[名前（Name）] フィールド	デバイスの名前。 （注） 一旦作成すると、デバイスの名前を変更することはできません。
[**State**] ドロップダウン リスト	BIOS によるデバイスの可視性。次のいずれかになります。 • [有効（Enabled）] : デバイスはブート順の設定で BIOS から認識できます。 • [無効（Disabled）] : デバイスはブート設定で BIOS から認識できません。
[Order]フィールド	デバイスの使用可能なリストにおけるそのデバイスの順序。 1 から n の間の数字を入力します（n はデバイスの数）。
[Slot] フィールド	デバイスが装着されているスロット。使用可能な範囲のスロット番号を入力します。
[Slot] フィールド	デバイスが装着されているスロット。範囲は C シリーズ サーバーに依存します。 • C220 M4 および C240 M4 サーバーの場合は、「HBA」を入力します。 • C460 M4 サーバの場合、1 ～ 255 の範囲の値または SAS を入力します。 • 他の C シリーズ サーバの場合、1 ～ 255 の範囲の値または M を入力します。
[**Add Device**] ボタン	[**Boot Order**] テーブルにデバイスを追加します。

名前	説明
[Cancel]ボタン	ダイアログボックスが開いているときに行われた変更を保存せずにダイアログボックスを閉じます。

PXE デバイスを追加するには、[**Add PXE**] をクリックし、次のパラメータを更新します。

名前	説明
[名前（Name）] フィールド	デバイスの名前。 この名前は、デバイスの作成後は変更できません。
[**State**] ドロップダウン リスト	BIOS によるデバイスの可視性。状態は次のいずれかになります。 • [有効（Enabled）] : デバイスはブート順の設定で BIOS から認識できます。 • [無効（Disabled）] : デバイスはブート順の設定で BIOS から認識できません。
[Order]フィールド	デバイスの使用可能なリストにおけるそのデバイスの順序。 1 から n の間の数字を入力します（n はデバイスの数）。
[Slot] フィールド	• C220 M4 および C240 M4 サーバでは、1 から 255 の間の数字、L、または MLOM を入力します。 • C3160 サーバでは 1 から 255 の間の値を入力します。 • C460M4 サーバでは 1 から 255 の間の値、L1 または L2 を入力します。 • 他の C シリーズ サーバーの場合は、0 ～ 255 の値または「L」を入力します。
MAC アドレス	ネットワーク イーサネット インターフェイスの MAC アドレス。 （注） このオプションを使用できるのは一部の C シリーズ サーバーだけです。
[Slot] フィールド	デバイスが装着されているスロット。使用可能な範囲のスロット番号を入力します。
[Port] フィールド	デバイスが装着されているスロットのポート。 0 ～ 255 の範囲内の数を入力してください。

SAN ブート デバイスを追加するには、**[SANブートの追加（Add SAN Boot）]** をクリックし、次のパラメータを更新します。

名前	説明
[名前（Name）] フィールド	デバイスの名前。 この名前は、デバイスの作成後は変更できません。
[**State**] ドロップダウン リスト	BIOS によるデバイスの可視性。状態は次のいずれかになります。 • [有効（Enabled）] : デバイスはブート順の設定で BIOS から認識できます。 • [無効（Disabled）] : デバイスはブート順の設定で BIOS から認識できません。
[Order]フィールド	デバイスの使用可能なリストにおけるそのデバイスの順序。 1 から n の間の数字を入力します（n はデバイスの数）。
[Slot] フィールド	デバイスが装着されているスロット。範囲は C シリーズ サーバに依存します。 • C220 M4 および C240 M4 サーバでは、1 から 255 の間の数字または MLOM を入力します。 • C460M4 サーバでは 1 から 255 の間の値、L1 または L2 を入力します。 • 他の C シリーズ サーバーの場合は、1 ～ 255 の値を入力します。
[Slot] フィールド	デバイスが装着されているスロット。使用可能な範囲のスロット番号を入力します。
[**LUN**] フィールド	デバイスが装着されているスロットの論理ユニット。 0 ～ 255 の範囲内の数を入力してください。
[変更を保存（Save Changes）] ボタン	[ブート順序（Boot Order）] テーブルにデバイスを追加し、変更を保存します。
[Cancel] ボタン	ダイアログボックスが開いているときに行われた変更を保存せずにダイアログボックスを閉じます。

iSCSI ブート デバイスを追加するには、**[iSCSIブートの追加（Add iSCSI Boot）]** をクリックし、次のパラメータを更新します。

名前	説明
[名前（Name）] フィールド	デバイスの名前。 この名前は、デバイスの作成後は変更できません。
[**State**] ドロップダウン リスト	BIOS によるデバイスの可視性。状態は次のいずれかになります。 • [有効（Enabled）] : デバイスはブート順の設定で BIOS から認識できます。 • [無効（Disabled）] : デバイスはブート順の設定で BIOS から認識できません。
[Order]フィールド	デバイスの使用可能なリストにおけるそのデバイスの順序。 1 から n の間の数字を入力します（n はデバイスの数）。
[Slot] フィールド	デバイスが装着されているスロット。範囲は C シリーズ サーバに依存します。 • C220 M4 および C240 M4 サーバでは、1 から 255 の間の数字、L、または MLOM を入力します。 • C3160 サーバでは 1 から 255 の間の値を入力します。 • C460M4 サーバでは 1 から 255 の間の値、L1 または L2 を入力します。 • 他の C シリーズ サーバーの場合は、1 ～ 255 の値または「L」を入力します。
[Slot] フィールド	デバイスが装着されているスロット。使用可能な範囲のスロット番号を入力します。
[Port] フィールド	デバイスが装着されているスロットのポート。 0 ～ 255 の範囲内の数を入力してください。 （注） VIC カードの場合は、ポート番号ではなく vNIC インスタンスを使用します。
[変更を保存（Save Changes）] ボタン	[ブート順序（Boot Order）] テーブルにデバイスを追加し、変更を保存します。
[Cancel] ボタン	ダイアログボックスが開いているときに行われた変更を保存せずにダイアログボックスを閉じます。

SD カードを追加するには、[**Add SD Card**] をクリックし、次のパラメータを更新します。

（注） このオプションは一部の UCS C シリーズのサーバでのみ利用可能です。

名前	説明
[名前（Name）] フィールド	デバイスの名前。 この名前は、デバイスの作成後は変更できません。
[**State**] ドロップダウン リスト	BIOS によるデバイスの可視性。次のいずれかになります。 • [有効（Enabled）] : デバイスはブート順の設定で BIOS から認識できます。 • [無効（Disabled）] : デバイスはブート設定で BIOS から認識できません。
[Order]フィールド	デバイスの使用可能なリストにおけるそのデバイスの順序。 1 から n の間の数字を入力します（n はデバイスの数）。
[変更を保存（Save Changes）] ボタン	[**Boot Order**] テーブルにデバイスを追加します。
[Cancel]ボタン	ダイアログボックスが開いているときに行われた変更を保存せずにダイアログボックスを閉じます。

USB デバイスを追加するには、[**Add USB**] をクリックし、次のパラメータを更新します。

名前	説明
[名前（Name）] フィールド	デバイスの名前。 この名前は、デバイスの作成後は変更できません。
[**Sub Type**] ドロップダウン リスト	特定のデバイス タイプの下位のサブデバイス タイプ。次のいずれかになります。 • **[CD]** • **[FDD]** • **[HDD]**
[**State**] ドロップダウン リスト	BIOS によるデバイスの可視性。次のいずれかになります。 • [有効（Enabled）] : デバイスはブート順の設定で BIOS から認識できます。 • [無効（Disabled）] : デバイスはブート順の設定で BIOS から認識できません。
[Order]フィールド	デバイスの使用可能なリストにおけるそのデバイスの順序。 1 から n の間の数字を入力します（n はデバイスの数）。

名前	説明
[変更を保存（Save Changes）] ボタン	[**Boot Order**] テーブルにデバイスを追加します。
[Cancel]ボタン	ダイアログボックスが開いているときに行われた変更を保存せずにダイアログボックスを閉じます。

仮想メディアを追加するには、[**Virtual Media**] をクリックし、次のパラメータを更新します。

名前	説明
[名前（Name）] フィールド	デバイスの名前。 この名前は、デバイスの作成後は変更できません。
[**Sub Type**] ドロップダウン リスト	特定のデバイス タイプの下位のサブデバイス タイプ。これは、次のいずれかになります。 • **[KVM Mapped DVD]** • **Cisco IMC マップされた DVD** • **[KVM Mapped HDD]** • **Cisco IMC マップされた HDD** • **[KVM Mapped FDD]**
[**State**] ドロップダウン リスト	BIOS によるデバイスの可視性。状態は次のいずれかになります。 • [有効（Enabled）] : デバイスはブート順の設定で BIOS から認識できます。 • [無効（Disabled）] : デバイスはブート順の設定で BIOS から認識できません。
[Order]フィールド	デバイスの使用可能なリストにおけるそのデバイスの順序。 1 から n の間の数字を入力します（n はデバイスの数）。
[変更を保存（Save Changes）] ボタン	[Boot Order] テーブルにデバイスを追加します。
[取り消し（Cancel）] ボタン	ダイアログボックスが開いているときに行われた変更を保存せずにダイアログボックスを閉じます。

PCH ストレージ デバイスを追加するには、[**PCH Storage**] をクリックし、次のパラメータを更新します。

名前	説明
[名前（Name）] フィールド	デバイスの名前。 この名前は、デバイスの作成後は変更できません。
[**State**] ドロップダウン リスト	BIOS によるデバイスの可視性。次のいずれかになります。 • [有効（Enabled）] : デバイスはブート順の設定で BIOS から認識できます。 • [無効（Disabled）] : デバイスはブート順の設定で BIOS から認識できません。
[Order]フィールド	デバイスの使用可能なリストにおけるそのデバイスの順序。 1 から n の間の数字を入力します（n はデバイスの数）。
[LUN] フィールド	デバイスが装着されているスロットの論理ユニット。 • 0 から 255 までの数字を入力します。 • AHCI モードの SATA：1 から 10 までの値を入力します。 • SWRAID モードの SATA：SATA の場合は 0、SATA の場合は 1 を入力します。 （注） SATA モードを使用できるのは一部の UCS C シリーズ サーバーだけです。
[変更を保存（Save Changes）] ボタン	[**Boot Order**] テーブルにデバイスを追加します。
[Cancel]ボタン	ダイアログボックスが開いているときに行われた変更を保存せずにダイアログボックスを閉じます。

UEFI シェル デバイスを追加するには、[Add UEFI Shell] をクリックし、次のパラメータを更新します。

名前	説明
[名前（Name）] フィールド	デバイスの名前。 この名前は、デバイスの作成後は変更できません。

名前	説明
[**State**] ドロップダウン リスト	BIOS によるデバイスの可視性。状態は次のいずれかになります。 • [有効（Enabled）] : デバイスはブート順の設定で BIOS から認識できます。 • [無効（Disabled）] : デバイスはブート順の設定で BIOS から認識できません。
[Order]フィールド	デバイスの使用可能なリストにおけるそのデバイスの順序。 1 から n の間の数字を入力します（n はデバイスの数）。
[**Add Device**] ボタン	[**Boot Order**] テーブルにデバイスを追加します。
[Cancel]ボタン	ダイアログボックスが開いているときに行われた変更を保存せずにダイアログボックスを閉じます。

HTTP ブート デバイス デバイスを追加するには、**[HTTPブートの追加（Add HTTP Boot）]** をクリックし、次のパラメータを更新します：

（注） HTTP ブート デバイスでは、次の OS（ISO）がサポートされています：

- SLES 12.x
- RHEL 8.2
- ESX 6.5

次の OS（ISO）は、HTTP ブート デバイスではサポートされていません：

- Windows 2016
- Windows 2019

名前	説明
[名前（Name）] フィールド	デバイスの名前。 この名前は、デバイスの作成後は変更できません。 1 ～ 30 文字の英数字、-（ハイフン）、_（アンダースコア）を入力できます。名前をハイフンまたはアンダースコアで始めることはできません。

名前	説明
[**State**] ドロップダウン リスト	BIOS によるデバイスの可視性。State には、次のいずれかを指定できます。 • **[有効（Enabled）]**—デフォルトオプション。デバイスはブート順の構成で BIOS から認識できます。 • [**Disabled**]：デバイスはブート順の設定で BIOS から認識できません。
[Order]フィールド	デバイスの使用可能なリストにおけるそのデバイスの順序。デフォルトのオプションは、 1 です。
[MAC Address] フィールド	ネットワーク イーサネット インターフェイスの MAC アドレス。
[IP タイプ (IP Type)] ドロップダウン リスト	IP のタイプ。 ドロップダウン リストに表示されている次のいずれかのオプションを選択します： • なし • IPv4 • IPv6 デフォルト値は None です。
[Slot] フィールド	デバイスが装着されているスロット。使用可能な範囲のスロット番号を入力します。 以下のリストから必要な値を入力します。 • OCP • MLOM • L • 1 ～ 255 の範囲内のいずれかの数。
[Port] フィールド	デバイスが装着されているスロットのポート。 0 ～ 255 の範囲内の数を入力してください。

名前	説明
[IP 構成タイプ (IP Config Type)] ドロップダウン リスト	IP 構成の種類。 ドロップダウンリストには、次のオプションが表示されます。 • **[なし（None）]** • **DHCP** • **[静的（Static）]** **DHCP** IP 構成の場合、選択した IP タイプに応じて、次のフィールドが表示されます： • MAC アドレス（MAC Address） • **IPタイプ** • **スロット** • **[ポート（Port）]** **静的** IP 構成の場合、選択した IP タイプに応じて、次のフィールドが表示されます： • **URI** • **IP Address** • **IPv4 ネットマスク**または **IPv6 ネットマスク** • **IPv4 ゲートウェイ**または **IPv6 ゲートウェイ** • **IPv4 優先 DNS サーバー**または **IPv6 優先 DNS サーバー**
URI フィールド	ユニフォーム情報技術識別子 HTTP サーバー パスの場所。 1ー255 文字の入力ができます。
[変更の保存（Save Changes）] ボタン	変更を保存し、デバイスを **ブート順序** 表に追加します。
[Cancel] ボタン	ダイアログボックスが開いているときに行われた変更を保存せずにダイアログボックスを閉じます。

UEFI セキュア ブートの概要

オペレーティング システムをロードし実行する前に、ロードおよび実行前のすべての EFI ドライバ、EFI アプリケーション、オプション ROM またはオペレーティング システムが確実に署名され信頼性と整合性が確認されるために、Unified Extensible Firmware Interface（UEFI）のセ

キュア ブートを使用できます。Web UI または CLI を使用して、このオプションをイネーブルにできます。UEFI のセキュア ブート モードをイネーブルにすると、ブート モードは UEFI モードに設定され、UEFI のブート モードがディセーブルになるまで、設定されているブート モードを変更できません。

（注） サポートされていない OS で UEFI セキュア ブートをイネーブルにすると、次の再起動時に、その特定の OS から起動することはできません。前の OS から起動しようとすると、Web UI のシステム ソフトウェア イベントの下にエラーが報告され記録されます。前の OS から起動するには、Cisco IMC を使用して UEFI セキュア ブート オプションをディセーブルにする必要があります。

重要 また、サポートされていないアダプタを使用すると、Cisco IMC SEL のエラー ログ イベントが記録されます。エラー メッセージが次のように表示されます。

System Software event: Post sensor, System Firmware error. EFI Load Image Security Violation. [0x5302] was asserted .

UEFI のセキュア ブートは次のコンポーネントでサポートされます。

コンポーネント	種類
サポートされている OS	• Windows Server 2019 • Windows Server 2016 • ESX 6.7 • ESX 6.5 • ESXi 7.0 • Linux
Broadcom PCI アダプタ	• 5709 デュアルおよびクアッド ポート アダプタ • 57712 10GBASE-T アダプタ • 57810 CNA • 57712 SFP ポート
Intel PCI アダプタ	• i350 クアッド ポート アダプタ • X520 アダプタ • X540 アダプタ • LOM

コンポーネント	種類
QLogic PCI アダプタ	• 8362 デュアル ポート アダプタ • 2672 デュアル ポート アダプタ
Fusion-io	
LSI	• LSI MegaRAID SAS 9240-8i • LSI MegaRAID SAS 9220-8i • LSI MegaRAID SAS 9265CV-8i • LSI MegaRAID SAS 9285CV-8e • LSI MegaRAID SAS 9285CV-8e • LSI MegaRAID SAS 9266-8i • LSI SAS2008-8i mezz • LSI Nytro カード

UEFI セキュア ブートのイネーブル化

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[コンピューティング（Compute）]メニューをクリックします。

ステップ 2 作業ウィンドウで **[BIOS]** タブをクリックします。

ステップ 3 **[ブート順序の設定（Configure Boot Order）]** タブの**[BIOS のプロパティ（BIOS Properties）]** 領域で、**[UEFI セキュア ブート（UEFI Secure Boot）]**チェックボックスをオンにします。

（注） オンにすると、ブート モードがUEFIセキュア ブートに設定されます。UEFIセキュア ブート オプションがディセーブルになるまで [**Configure Boot Mode**] は変更できません。

（注） RFD（Reset Factory Default）の場合は、UEFI セキュア ブートを再度有効にする必要があります。

サポートされていない OS で UEFI セキュア ブートをイネーブルにすると、次の再起動時に、その特定の OS から起動することはできません。前の OS から起動しようとすると、Web UI のシステム ソフトウェア イベントの下にエラーが報告され記録されます。前の OS から起動するには、Cisco IMC を使用して UEFI セキュア ブート オプションをディセーブルにする必要があります。

ステップ 4 **[Save Changes]**をクリックします。

次のタスク

サーバを再起動してコンフィギュレーション ブート モード設定を有効にします。

UEFI セキュア ブートのディセーブル化

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[コンピューティング（Compute）]メニューをクリックします。

ステップ 2 **作業ウィンドウで [BIOS]** タブをクリックします。

ステップ 3 [**BIOS Properties**] 領域で、[**UEFI Secure Boot**] チェックボックスをオフにします。

ステップ 4 **[Save Changes]**をクリックします。

次のタスク

サーバを再起動してコンフィギュレーション ブート モード設定を有効にします。

サーバーの実際のブート順の表示

サーバーの実際のブート順とは、サーバーが最後にブートされたときに BIOS によって実際に使用されたブート順です。実際のブート順は、Cisco IMC で設定されたブート順とは異なる場合があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[コンピューティング（Compute）]メニューをクリックします。

ステップ 2 [BIOS] タブで [Configure Boot Order] タブをクリックします。

ステップ 3 [BIOS Properties] 領域の [Configure Boot Order] をクリックします。

この領域には、Cisco IMC を介して設定されたブート順のデバイスと、サーバー BIOS によって使用される実際のブート順が表示されます。

[設定されたブート デバイス（Configured Boot Devices）] セクションに、Cisco IMC で設定されているブート順序（**[基本（Basic）]** または **[詳細設定（Advanced）]**）が表示されます。この設定が変更されると、次回のサーバ ブート時に、Cisco IMC から BIOS にこのブート順序が送信されます。基本設定では、デバイス タイプのみを指定できます。[詳細設定（Advanced）]

設定では、スロット、ポート、および LUN などの特定のパラメータを使用してデバイスを設定できます。

設定済みのブート順序を変更する場合、または以前に設定されていたブート順序を復元する場合は、[ブート順序の設定（Configure Boot Order）] ボタンをクリックします。これらの変更を直ちに適用するには、サーバを再起動する必要があります。[BIOS] タブを更新すると、新しいブート順序を確認できます。

（注） この情報は、次回のサーバーのブート時に BIOS にのみ送信されます。設定が変更されるまでは、Cisco IMC から BIOS に再びブート順序の情報が送信されることはありません。

[Actual Boot Devices] セクションには、サーバーが最後にブートされたときに BIOS によって実際に使用されたブート順が表示されます。次のいずれかの条件が発生すると、実際のブート順は設定されたブート順と異なります。

- 設定されたブート順を使用してブートしようとしたときに BIOS で問題が発生した。
- ユーザーが BIOS で直接、ブート順を変更した。手動による変更をオーバーライドするには、Cisco IMC を使用して設定済みブート順序を変更してから、サーバを再起動します。

（注） 設定されたブート順を使用して新しいポリシーを作成すると、BIOS はこの新しいポリシーをシステムに存在するデバイス（複数の場合あり）にマッピングしようとします。[実際のブート順序（Actual Boot Order）] エリアに、マッピングされた実際のデバイス名とポリシー名が表示されます。BIOS が Cisco IMC で特定のポリシーをマッピングするデバイスを見つけられない場合、[実際のブート順序（Actual Boot Order）] エリアでは実際のデバイス名が [NonPolicyTarget] として表示されます。

1 回限りのブート デバイスを使用してブートするサーバの設定

現在設定されているブート順序を乱さずに、次回のサーバブートに限り特定のデバイスから起動するように、サーバを設定できます。1 回限りのブート デバイスからサーバがブートしたら、その後のリブートはすべて以前に設定されていたブート順序で実行されます。

始める前に

サーバのブート順を設定するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [コンピューティング（Compute）] メニューをクリックします。

ステップ 2 [BIOS] タブで [Configure Boot Order] タブをクリックします。

ステップ 3 [BIOS Properties] 領域で、[Configured One Time Boot Device] ドロップダウンからオプションを選択します。

（注） 拡張ブートデバイスを無効にしてホストが設定されている場合でも、ホストは1回限りのブート デバイスにブートします。

サーバ アセット タグの作成

始める前に

このタスクを実行するには、user または admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。
ステップ 2 [シャーシ（Chassis）] メニューで [サマリー（Summary）] をクリックします。
ステップ 3 [Server Properties] 領域で、[Asset Tag] フィールドを更新します。
ステップ 4 **[Save Changes]**をクリックします。

電力ポリシーの設定

電力制限

重要 このセクションは、一部の UCS C シリーズのサーバでのみ利用可能です。

パワー キャッピングによって、サーバの電力消費をアクティブに管理する方法が決定されます。パワーキャッピングオプションを有効にすると、システムにより電力消費がモニタされ、割り当てられている電力制限を超えないように電力が維持されます。サーバが電力制限を維持できない場合、またはプラットフォームの電力を修正時間内に指定の電力制限に戻すことができない場合、**[電力プロファイル（Power Profile）]** 領域の **[アクション（Action）]**フィールドに指定したアクションがパワー キャッピングにより実行されます。

パワーキャッピングが有効になったら、定義された属性を持つ標準電力プロファイルまたは詳細電力プロファイルを使用できるように複数の電力プロファイルを設定できます。標準電力プロファイルを選択する場合は、電力制限、修正時間、修正アクション、中断期間、ハードキャップ、ポリシー状態（有効な場合）を設定できます。詳細電力プロファイルを選択する場合は、

標準電力プロファイルの属性の他に、ドメイン固有の電力制限、安全スロットル レベル、周囲温度に基づくパワー キャッピング属性も設定できます。

（注） 次に示す変更は、Cisco UCS C シリーズ リリース 2.0(13) 以降に適用されます。

- 2.0(13) リリースへのアップグレード後、ホストの電源を初めてオンにするときに、電力特性評価が自動的に実行されます。それ以降は、電力特性評価は**[電力特性評価の実行（Run Power Characterization）]**セクションで指定されているとおりに開始する場合にのみ実行されます。
- また、サーバへの電源再投入が行われ、CPU または DIMM の設定が変更されている場合にも、初回ホスト ブート時に電力特性評価が自動的に実行されます。PCIe アダプタ、GPU、HDD などのハードウェアが変更されている場合は、電力特性評価は実行されません。特性評価された電力範囲は、ホストの電源再投入後に存在するコンポーネントに応じて変更されます。

Web UI の **[パワー キャッピング設定（Power Cap Configuration）]** タブの **[電力特性評価の実行（Run Power Characterization）]**オプションを選択すると、ホストの電源が再投入され、電力特性評価が開始されます。

電源の冗長性ポリシーの設定

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 [シャーシ（Chassis）] メニューで [センサー（Sensors）] をクリックします。

ステップ 3 [Sensors] 作業領域で、[Power Supply] タブをクリックします。

ステップ 4 電源装置の次のセンサー プロパティを確認します。

[プロパティ（Properties）] 領域

名前	説明
[Redundancy Status] フィールド	電源装置の冗長性のステータス。

名前	説明
[冗長性ポリシー（Redundancy Policy）] フィールド	電源装置の冗長性のポリシー。次のいずれかになります。 • [非冗長] : N（使用可能なPSU出力性能）は、インストールされているPSUの数に等しくなります。この場合、PSUのエラー、またはグリッドのエラーはサポートされません。 • [N+1] : N（使用可能なPSU出力性能）は、インストールされている PSU の数から 1 を引いた数に等しくなります。この場合、単一の PSU のエラーはサポートされますが、グリッドのエラーはサポートされません。 • [グリッド（Grid）] : N（使用可能なPSU出力性能）は、インストールされている PSU の数の半分に等しくなります。この場合、N 個の PSU のエラー、またはグリッドのエラーがサポートされます。このポリシーは、N個のPSUを 1 つのフィードに接続し、別の N 個の PSU を別のフィードに接続したことを暗黙的に示しています。

電力特性評価の有効化

電力特性評価を有効にできるのは、一部の Cisco UCS C シリーズ サーバーだけです。

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 **[シャーシ（Chassis）]**メニューで **[電源管理（Power Management）]** をクリックします。

ステップ 3 [Power Cap Configuration] タブで、[Run Power Characterization] リンクをクリックします。

現在の電力状態に応じてホストの電源がオンになるかまたは再起動することを通知する確認ボックスが表示されます。メッセージを確認してから **[OK]** をクリックしてダイアログボックスを閉じます。

[ステータス（Status）] フィールドで、電力特性評価の進行状況を確認できます。ステータスは、次のいずれかになります。

- **[未実行（Not Run）]**：工場出荷時のデフォルトにリセットされてから、電源特性評価は一度も実行されていません。

- **[実行中（Running）]**：電源特性評価プロセスが進行中です。
- **[完了（Completed Successfully）]**：電源特性評価は正常に実行されました。
- **[デフォルトの使用（Using Defaults）]**：電源特性評価の実行完了後、システムが有効な値を取得できなかった場合は、パワーキャッピングの推奨される最小電力および最大電力としてデフォルト値を使用します。

  電力特性評価の操作の実行後、プラットフォームの電力制限の範囲が最小および最大電力としてワット単位で [Recommended Power Cap] 領域の下に読み込まれます。

  パワー キャッピング制限の 3 つの値が表示されます。[最小値（スロットリングを許可）（Minimum (Allow Throttling)）]、[最小値（効率的）（Minimum (Efficient)）]、および [最大値（Maximum）]。

  - [最小値（スロットリングを許可）]：CPU のスロットリングが有効になっている場合のシャーシの電力の下限です。

    （注） この最小電力の下限値は、[スロットルを許可（Allow Throttle）] チェックボックスがオンになっているときにのみ使用できます。

  - [最小値（効率的）]：CPU のスロットリングが無効になっている場合のシャーシの電力の下限です。
  - [最大値（Maximum）]：シャーシの電力の上限です。

パワー キャッピングの有効化

このオプションを使用できるのは一部の Cisco UCS C シリーズ サーバーだけです。

始める前に

- このタスクを実行するには、admin権限を持つユーザとしてログインする必要があります。
- 電力特性評価を実行します。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 **[シャーシ（Chassis）]**メニューで **[電源管理（Power Management）]** をクリックします。

ステップ 3 [Power Capping] チェックボックスをオンにします。

（注） これは、パワーキャッピングを有効または無効にするグローバル オプションです。電力プロファイル設定を指定するには、このオプションを有効にする必要があります。

ステップ 4 [Save Changes] をクリックします。

[電源プロファイル（Power Profiles）]

複数のプロファイルを設定し、属性を設定できます。プロファイルは Web UI または CLI のいずれかを使用して設定します。Web UI では、プロファイルは [Power Capping] 領域の下にリストされます。CLI で、**power-cap-config** コマンドを入力するとプロファイルが設定されます。電力制限機能に関する次の電力プロファイルを設定できます。

- [標準（Standard）]：プラットフォーム ドメインの電力制限を設定できます。
- [詳細（Advanced）]：さまざまな属性（電力制限ポリシー、フェールセーフ電力制限ポリシー、周囲温度に基づく電力制限ポリシーなど）を設定できます。

標準電力プロファイルの設定

このオプションを使用できるのは一部の Cisco UCS C シリーズ サーバーだけです。

始める前に

- パワー キャッピングを有効にする必要があります。
- このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 **[シャーシ（Chassis）]**メニューで **[電源管理（Power Management）]** をクリックします。

ステップ 3 [Power Profiles] 領域で、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	電力制限の属性を設定するために選択されたプロファイルの名前。
[プロファイルを有効にする（Enable Profile）] チェックボックス	電源プロファイルの編集を有効にします。
[スロットルの許可（Allow Throttle）] チェックボックス	オンにした場合、プロセッサがより積極的な電源管理メカニズム、たとえば、通常の内部メカニズムに加えて、電力制限を維持するための CPU スロットリング状態（T 状態）やメモリ帯域幅スロットリングなどを使用するようにします。

名前	説明
[訂正時間（Correction Time）] フィールド	[Action] フィールドで指定したアクションが実行される前に、プラットフォームの電力が指定された電力制限に戻る必要のある時間（秒単位）。 範囲は、1 ～ 600 です。 この範囲はサーバの PSU 値によって異なります。 （注） すべての PSU モデルでサポートされている最小訂正時間は 1 秒です。ただし、DPST-1400AB モデルと DPST-1200DB PSU モデルの場合の最小訂正時間は 3 秒です。
[アクション（Action）] ドロップダウン リスト	指定した電力制限が修正用時間内に維持されない場合に実行されるアクション。 • **[アラート（Alert）]**—イベントをシスコ IMC SEL に記録します。 • **[アラートおよびシャットダウン（Alert and Shutdown）]**—イベントをシスコ IMC SEL に記録し、ホストを正規の手順でシャットダウンします。
[電力上限（Power Limit）] チェックボックス	サーバの電力上限。 指定された範囲内での電力を入力します（ワット数）。
[Set Hard Cap] チェックボックス	オンにした場合、設定されている電力制限値を超えてプラットフォーム消費が発生することはないことが保証されます。プラットフォーム電力消費は、構成されている電力制限値より下の安全なオフセット マージンに維持されます。

ステップ 4 [Save Changes] をクリックします。

詳細電力プロファイルの設定

このオプションを使用できるのは一部の Cisco UCS C シリーズ サーバーだけです。

始める前に

- パワー キャッピングを有効にする必要があります。
- このタスクを実行するには、admin権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 **[シャーシ（Chassis）]**メニューで **[電源管理（Power Management）]** をクリックします。

ステップ 3 [Power Cap Configuration] タブの [Power Profiles] テーブルから、[Advanced] プロファイルを選択します。
標準プロファイル設定の他に、**[ドメイン固有の電力制限（Domain Specific Power Limit）]**、**[安全スロットル レベル（Safe Throttle Level）]**、および **[周囲温度ベースのパワー キャッピング（Ambient Temperature Based Power Capping）]**領域が表示されます。

ステップ 4 [Domain Specific Power Limit] 領域で、次のフィールドに値を入力します。

名前	説明
[CPU] フィールド	CPU の電力上限。 指定された範囲内での電力を入力します（ワット数）。
[メモリ]フィールド	メモリの電力上限。 指定された範囲内の電力（ワット単位）を入力します。 （注） このフィールドは、Intel® Optane™ DC 永続メモリ モジュールを搭載したサーバでは使用できません。
[Platform] フィールド	プラットフォームの電力上限。 指定された範囲内での電力を入力します（ワット数）。

ステップ 5 [Suspend Period] 領域で、[Configure] をクリックして、中断期間を特定の期間と日付に設定します。

ステップ 6 [Safe Throttle Level] 領域で、次のフィールドに値を入力します。

名前	説明
[フェールセーフタイムアウト（Failsafe Timeout）] フィールド	内部障害（プラットフォームやCPUの電力測定値の欠如など）がパワー キャッピングに影響を及ぼしている場合に適用される、安全なスロットル ポリシー。 値（秒単位）を入力します。
[CPU] フィールド	CPU のスロットリング レベル。 範囲は、0から100までです（パーセント）。
[メモリ]フィールド	メモリのスロットリング レベル。 範囲は、0から100までです（パーセント）。
[プラットフォーム（Platform）] フィールド	プラットフォームのスロットリング レベル。 範囲は、0から100までです（パーセント）。

ステップ 7 **[周囲温度ベースのパワー キャッピング（Ambient Temperature Based Power Capping）]**領域で、次のフィールドに値を入力します。

名前	説明
[プラットフォーム温度トリガー（Platform Temp Trigger）] フィールド	インレット（前面パネル）温度センサー値（摂氏）。 （注） プラットフォームのインレット温度が指定された上限を超えると、システムは温度による電力制限値をパワーキャッピング上限として使用します。
[温度による電力制限（Thermal Power Limit）] フィールド	維持する電力制限（ワット単位）。

ステップ 8 [Save Changes] をクリックします。

電力プロファイルのデフォルトへのリセット

このオプションを使用できるのは一部の Cisco UCS C シリーズ サーバーだけです。

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 **[シャーシ（Chassis）]**メニューで **[電源管理（Power Management）]** をクリックします。

ステップ 3 [Power Profiles] 領域で、[Reset Profiles to Default] ボタンをクリックします。

（注） この操作により、すべての電力プロファイル設定が工場出荷時のデフォルト値にリセットされ、パワー キャッピングが無効になります。

ステップ 4 [Save Changes] をクリックします。

電力モニタリング

電力モニタリングは、ホストの電源がオンになる時点またはホストが起動する時点から開始します。この機能は、プラットフォーム、CPU、メモリ ドメインから電力消費に関する統計情報を収集し、収集期間における最小測定値、最大測定値、および平均測定値を提供します。これらの計測値を使用して、ドメインの電力消費トレンドを計算できます。Cisco IMC は、さまざまな期間（時間、日、週など）のグラフをプロットするため、この電力消費統計値を収集して保存します。

（注） 追加で統計情報収集ポリシーを作成することはできません。また、既存のモニタリング ポリシーは削除できません。デフォルト ポリシーを変更することだけが可能です。

電力モニタリングの概要の表示

このオプションを使用できるのは一部の Cisco UCS C シリーズ サーバーだけです。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 **[シャーシ（Chassis）]**メニューで **[電源管理（Power Management）]** をクリックします。

ステップ 3 [作業（Work）] ペインで、[電力モニタリング（Power Monitoring）] タブをクリックします。

ステップ 4 [電力モニタリングの概要（Power Monitoring Summary）] 領域で、次の情報を確認します。

次の表に、最後にリブートされてからシステムとそのコンポーネントによって消費された電力が表示されます。

名前	説明
[Monitoring Period]	システムが最後にリブートされてから現在までのシステムの消費電源モニタリング時間。 モニタリング期間は、日付と HH:MM:SS という形式で表示されます。

（注） **[シャーシ (Chassis)]** の下に **[モニタリング期間 (Monitoring Period)]** が表示されます。

プラットフォーム、**CPU**、および**メモリ**領域は、**サーバ 1** および**サーバ 2** で使用できます。

ステップ 5 [Platform] 領域で、次の情報を確認します。

名前	説明
現在（Current）	現在サーバ、CPU、メモリで使用されている電力（ワット単位）。
[Minimum]	システムが最後にリブートされてから現在までにサーバ、CPU、およびメモリで使用された最小ワット数。
[Maximum]	システムが最後にリブートされてから現在までにサーバ、CPU、およびメモリで使用された最大ワット数。
[Average]	定義された期間におけるサーバ、CPU、およびメモリの平均消費電力量（ワット）。

ステップ 6 [CPU] 領域で、次の情報を確認します。

名前	説明
現在（Current）	現在 CPU で使用されている電力（ワット単位）。
[Minimum]	最後にリブートされてから現在までに CPU で使用された最小ワット数。
[Maximum]	最後にリブートされてから現在までに CPU で使用された最大ワット数。
[Average]	定義された期間におけるサーバ、CPU、およびメモリの平均消費電力量（ワット）。

ステップ 7 [Memory] 領域で、次の情報を確認します。

名前	説明
現在（Current）	現在メモリで使用されている電力（ワット単位）。

名前	説明
[Minimum]	最後にリブートされてから現在までにメモリで使用された最小ワット数。
[Maximum]	最後にリブートされてから現在までにメモリで使用された最大ワット数。
[Average]	定義された期間におけるメモリの平均消費電力量（ワット単位）。

ステップ 8 [Chart Properties] 領域で、グラフ、コンポーネントを確認および更新し、消費電力の詳細を表示します。

名前	説明
[Chart Settings]	チャート プロパティおよびチャートでのデータ表示方法を設定できます。
電力統計情報とサーバー使用率データのダウンロード（Download Power Statistics and Server Utilization Data）	電源統計情報およびホスト サーバの使用状況に関する情報をダウンロードできます。ファイルはローカル ダウンロード フォルダにダウンロードされます。 （注） ダウンロード済みの統計情報ファイルのサイズが256 KB未満の場合、ファイルをダウンロードすると、既存のファイルとは別に、電源統計情報のファイルとホストサーバ使用状況に関する情報のファイルのセットがダウンロードされます。既存のファイルのサイズが 256 KB を超えている場合は、次のファイルセットによって既存のファイルが上書きされます。

名前	説明
[チャート（Chart）] ドロップダウン リスト	選択した期間における各サーバの電力消費傾向を収集できます。次のいずれかになります。 • **過去 1 時間**：5 分おきのグラフを作成します。 • **過去 1 日**：現在の時刻から毎時間のグラフを作成します。 • **過去 1 週間**：毎日のグラフを作成します。

名前	説明
[Component] ドロップダウン リスト	選択した期間の消費電力を表示する対象のコンポーネント。次のいずれかになります。 • **シャーシ** • ***Server 1*** • ***Server 2***
[Domain] ドロップダウン リスト	表示されるデフォルト値は **Platform**です。
[Plot] ボタン	選択したコンポーネントの指定した期間の消費電力が表示されます。
[チャート/テーブル] ビュー（マウスのカーソルを合わせると表示されます）	電源モニタリング サマリを [チャート（Chart）] ビューまたは [テーブル（Table）] ビューのどちらで表示するかを選択します。
[チャート タイプ（Chart Type）]（マウスのカーソルを合わせると表示されます）	表示するチャートのタイプを選択します。次のいずれかを選択できます。 • [折れ線グラフ（Line Chart）]：電力モニタリング データが折れ線グラフで表示されます。 • [縦棒グラフ（Column Chart）]：電力モニタリング データが縦棒グラフで表示されます。 **デフォルトのグラフ**：折れ線グラフです。 （注） [グラフ（Chart）] ドロップダウン リストで [先週（Last Week）] が選択され、複数のコンポーネントが選択された場合、縦棒グラフは表示されず、デフォルトで折れ線グラフが表示されます。このようなシナリオでは、次のメッセージが表示されます。選択した設定では、縦棒グラフをプロットすることはできません。折れ線グラフに戻ります。
[現在（Current）] 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、選択した期間における、選択したコンポーネントの現在の消費電力量がチャートに表示されます。

名前	説明
[平均（Average）] 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、選択した期間における、選択したコンポーネントの平均消費電力量がプロットに表示されます。
[最大（Maximum）] 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、選択した期間における、選択したコンポーネントの最大消費電力量（ワット単位）がプロットに表示されます。
[最小（Minimum）] 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、選択した期間における、選択したコンポーネントの最小消費電力量（ワット単位）がプロットに表示されます。

チャートでの電力統計の表示

このオプションを使用できるのは一部の Cisco UCS C シリーズ サーバーだけです。

始める前に

- パワー キャッピングを有効にする必要があります。
- このタスクを実行するには、admin権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 **[シャーシ（Chassis）]**メニューで **[電源管理（Power Management）]** をクリックします。

ステップ 3 [作業（work）] ペインで、[電力モニタリング（Power Monitoring）] タブをクリックします。

ステップ 4 [Power Monitoring] タブで、チャートとコンポーネントを確認して更新し、電力消費の詳細を確認します。

名前	説明
[チャート（Chart）] ドロップダウン リスト	選択した期間における各サーバの電力消費傾向を収集できます。次のいずれかになります。 • [過去 1 時間（Last One Hour）] : 5 分間隔のチャートをプロットします。 • [過去 1 日（Last One Day）] : 現在時刻から 1 時間間隔のチャートをプロットします。 • [過去 1 週間（Last One Week）] : 1 日間隔のチャートをプロットします。
[コンポーネント（Component）] ドロップダウン リスト	選択した期間の消費電力を表示する対象のコンポーネント。次のいずれかになります。 • **Platform** • **CPU** • **メモリ** • **すべて**
[最大（Maximum）] 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、選択した期間における、選択したコンポーネントの最大消費電力量（ワット単位）がプロットに表示されます。
[最小（Minimum）] チェックボックス	オンにすると、選択した期間に選択したコンポーネントが消費した最小ワット数がグラフに表示されます。
[平均（Average）] チェックボックス	オンにすると、選択した期間に選択したコンポーネントが消費した平均電力量がグラフに表示されます。
[現在（Current）] チェックボックス	オンにすると、選択した期間に選択したコンポーネントが消費した現在の電力がグラフに表示されます。
[Plot] ボタン	指定した期間に選択したコンポーネントが消費した電力が表示されます。

電力測定値チャートに、選択されている期間における各種コンポーネントの電力消費値がプロットされます。これらの電力消費値は、ホストの電源がオンになった時点から取り込まれます。電力プロファイルが有効な場合、チャートには電力制限が赤色の線としてプロットされま

す。このプロットから、システムの電力消費トレンドを確認できます。特定のドメインに設定されている電力制限値を確認するには、これらのトレンド線にマウスを移動します。

標準プロファイルを選択する場合、トレンド線は電力制限を示します。詳細プロファイルを選択する場合、電力プロファイル設定に応じてトレンド線はCPU、メモリ、およびプラットフォームの電力制限を示します。

（注） [Power Cap Configuration] タブでプロファイルが無効な場合は、トレンド線は表示されません。

ステップ 5 [Save Changes] をクリックします。

電力統計とサーバ使用率データのダウンロード

このオプションを使用できるのは一部の Cisco UCS C シリーズ サーバーだけです。

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 **[シャーシ（Chassis）]**メニューで **[電源管理（Power Management）]** をクリックします。

ステップ 3 [作業（Work）] ペインで、[電力モニタリング（Power Monitoring）] タブをクリックします。

ステップ 4 **[電力モニタリング（Power Monitoring）]** タブで **[電力統計とサーバ使用率データのダウンロード（Download Power Statistics and Server Utilization Data）]** をクリックします。

ファイルはローカル ダウンロード フォルダにダウンロードされます。

（注） ダウンロード済みの統計情報ファイルのサイズが 256 KB 未満の場合、ファイルをダウンロードすると、既存のファイルとは別に、電源統計情報のファイルとホストサーバ使用状況に関する情報のファイルのセットがダウンロードされます。既存のファイルのサイズが 256 KB を超えると、次のファイルのセットが既存のファイルを上書きします。

電力復元ポリシーの設定

電力復元ポリシーによって、シャーシの電力供給が失われた後、サーバーに電力を復元する方法が決定されます。

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[コンピューティング（Compute）]メニューをクリックします。

ステップ 2 作業ウィンドウで**[電源ポリシー（Power Policies）]**タブをクリックします。

ステップ 3 [Power Restore Policy] 領域で、次のフィールドを更新します。

名前	説明
[電力復元ポリシー（Power Restore Policy）] ドロップダウン リスト	予期しない電源損失後、シャーシ電源が復元されたときに実行されるアクション。次のいずれかになります。 • [電源オフ（Power Off）]：手動で再起動されるまで、サーバーはオフのままです。 • [電源オン（Power On）]：電源が復元されたときに、サーバーは通常どおりに起動できます。サーバーはただちに再起動できますが、任意で一定の遅延またはランダムな遅延後に再起動することもできます。 • [最後の状態を復元（Restore Last State）]：サーバーが再起動し、システムは電源喪失前に実行されていたプロセスの復元を試みます。

ステップ 4 [Save Changes] をクリックします。

ファン ポリシーの設定

ファン制御ポリシー

ファン制御ポリシーを使ってファンの速度を制御することにより、サーバの消費電力を削減し、ノイズ レベルを下げることができます。これらのファン ポリシーが導入される前は、いずれかのサーバコンポーネントの温度が設定済みしきい値を超過した場合に、ファン速度が自動的に増加しました。ファン速度を低く抑えるために、通常、コンポーネントのしきい値温度を高い値に設定しました。この動作はほとんどのサーバ構成に最適でしたが、次のような状況に対処できませんでした。

- 最大の CPU パフォーマンス

高パフォーマンスを得るには、いくつかの CPU を設定済みしきい値よりもかなり低い温度に冷却する必要があります。これは非常に高速なファン速度を必要とし、結果として電力消費とノイズ レベルが増大しました。

- 低電力消費

  電力消費を最も低く抑えるにはファンを非常に遅くする必要があり、場合によっては、ファン停止をサポートするサーバで完全に停止する必要があります。ただし、ファンの速度を遅くすると、結果としてサーバが過熱します。この状況を回避するには、可能な最低速度よりもやや速くファンを作動させる必要があります。

ファンポリシーを導入すると、サーバ内のコンポーネントに基づき、そのサーバに適したファン速度を決定できます。さらに、最大の CPU パフォーマンスと低消費電力に関連する問題に対処するために、ファン速度を設定することができます。

次のファン ポリシーの中から選択できます。

- [バランス（Balanced）]：この設定はほとんどのサーバー構成を冷却できますが、PCIe カードは容易に過熱するため、これらのカードのあるサーバーには適していない可能性があります。
- [パフォーマンス（Performance）]：この設定は、高パフォーマンスを得るために最高速度でファンを作動させる必要のあるサーバー構成に使用できます。この設定により、ファン速度は、Balanced ファン ポリシーで設定されたファン速度と同じ速度またはより高速で動作します。

（注） このオプションを使用できるのは一部の C シリーズ サーバーだけです。

- **[低電力（Low Power）]**：この設定は、PCIe カードが含まれない最小構成のサーバに最適です。
- **[高電力（High Power）]**：このポリシーは、容易に過熱して高温になる PCIe カードを含むサーバーに最適です。
- **[最大電力（Maximum Power）]**：この設定は、非常に高いファン速度を必要とするサーバー構成に使用できます。このポリシーは、容易に過熱して非常に高温になる PCIe カードを含むサーバに最適です。
- **Acoustic**：この設定は、ファンのノイズ レベルを設定するために使用できます。これにより、サーバのノイズ リダクションが可能になります。

  このポリシーを適用すると、システム パフォーマンスに影響するパフォーマンス スロットリングが発生する可能性があります。過剰な温度またはパフォーマンス イベントがイベント ログに記録されている場合は、**低電力**などの標準のファン制御ポリシーを選択します。これは、中断のない変更です。

（注） このオプションは、Cisco UCS C220 M5、C240 SD M5、C240 M5、C220 M6、C240 M6、C245 M6、C225 M6、C220 M7、および C240 M7 サーバーでのみ使用できます。 これらのサーバーでは、**[音響（Acoustic）]** がデフォルトのファン ポリシーです。

他のサーバーの場合、デフォルトのファンポリシーは、サーバー構成とサーバーに存在する PCIe カードの数によって異なります。

（注） Cisco UCS M5 サーバーの場合、Cisco IMC でファン ポリシーを設定することはできますが、実際のファン作動速度はサーバーの構成要件により決定されます。PCIe カードには、温度要件に応じて最小ファン速度のタグが付けられています。サーバーにこれらの PCIe カードが装備されている場合、タグ付けされた要件を下回るファンポリシーを構成することはできません。

[構成ステータス（Configuration Status）] には、Cisco UCS M5 サーバーで構成されたファンポリシーのステータスが表示されます。次のいずれかになります。

- [SUCCESS]：選択されたファンポリシーはサーバで実行されている実際のファン速度に一致します。
- [PENDING]：設定されたファンポリシーはまだ有効になっていません。この原因として、以下が考えられます。
  - サーバの電源がオフになっている
  - BIOS POST が完了していない
- [ファン ポリシーの上書き（FAN POLICY OVERRIDE）]：指定されたファン速度を、サーバーの設定要件によって決定された実際の速度で上書きします。

（注）
- Cisco UCS C220 M7、C240 M7、C220 M6、C240 M6、UCS C220 M5、C240 M5、C240 SD M5、C125 M5、C480 M5、C480-M5ML の場合、**[適用されるファン ポリシー（Applied fan policy）]** は、サーバーに存在する PCIe カードによって異なります。
- Cisco UCS C225 M6 および C245 M6 の場合、**[適用されるファン ポリシー（Applied fan policy）]** は、サーバーに存在する PCIe カードまたは特定の CPU タイプによって異なります。

ファン ポリシーの設定

サーバー設定およびサーバー コンポーネントに基づいて適切なファン ポリシーを決定できます。

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [コンピューティング（Compute）] メニューをクリックします。

ステップ 2 作業ウィンドウで**[電源ポリシー（Power Policies）]**タブをクリックします。

ステップ 3 [Configured Fan Policy] 領域で、ドロップダウン リストからファン ポリシーを選択します。次のいずれかを指定できます。

名前	説明
[ファン ポリシー（Fan Policy）] ドロップダウン リスト	

名前	説明
	次のいずれかになります。 • [バランス（Balanced）]：この設定はほとんどのサーバー構成を冷却できますが、PCIe カードは容易に過熱するため、これらのカードのあるサーバーには適していない可能性があります。 • [パフォーマンス（Performance）]：この設定は、高パフォーマンスを得るために最高速度でファンを作動させる必要のあるサーバー構成に使用できます。 この設定により、ファン速度は、Balanced ファン ポリシーで設定されたファン速度と同じ速度またはより高速で動作します。 （注） このオプションを使用できるのは一部の C シリーズ サーバーだけです。 • **[低電力（Low Power）]**：この設定は、PCIe カードが含まれない最小構成のサーバに最適です。 • **[高電力（High Power）]**：このポリシーは、容易に過熱して高温になる PCIe カードを含むサーバーに最適です。 • **[最大電力（Maximum Power）]**：この設定は、非常に高いファン速度を必要とするサーバー構成に使用できます。このポリシーは、容易に過熱して非常に高温になる PCIe カードを含むサーバに最適です。 • **Acoustic**：この設定は、ファンのノイズ レベルを設定するために使用できます。これにより、サーバのノイズ リダクションが可能になります。 このポリシーを適用すると、システム パフォーマンスに影響するパフォーマンス スロットリングが発生する可能性があります。過剰な温度またはパフォーマンス イベントがイベント ログに記録されている場合は、**低電力**などの標準のファン制御ポリシーを選択します。これは、中断

名前	説明
	のない変更です。 （注） このオプションは、Cisco UCS C220 M5、C240 SD M5、C240 M5、C220 M6、C240 M6、C225 M6、C245 M6、C220 M7、および C240 M7 サーバーでのみ使用できます。 Cisco UCS C シリーズ M6 サーバー、Cisco UCS C シリーズ M7 サーバー、および Cisco UCS C240 SD M5 サーバーの場合、**[アコースティック（Acoustic）]** がデフォルトのファン ポリシーです。 他のすべてのサーバーでは、デフォルトのファンポリシーは **[低電力（Low Power）]** です。

名前	説明
[Applied Fan Policy] フィールド	サーバ上で稼働するファンの実際の速度。 設定済みのファン ポリシーが有効になっていない場合は、[なし（N/A）]が表示されます。設定されたファン ポリシーは、サーバーの電源が入り、POST が完了すると有効になります。 （注） • Cisco UCS C220 M7、C240 M7、C220 M6、C240 M6、UCS C220 M5、C240 M5、C240 SD M5、C125 M5、C480 M5、C480-M5ML の場合、**[適用されるファン ポリシー（Applied Fan Policy）]** は、サーバーに存在する PCIe カードによって異なります。 • Cisco UCS C225 M6 および C245 M6 の場合、**[適用されるファン ポリシー（Applied Fan Policy）]** は、サーバーに存在する PCIe カードまたは特定のタイプの CPU によって異なります。

名前	説明
[Configuration Status] フィールド	ファン ポリシーの設定のステータス。次のいずれかになります。 • [成功（SUCCESS）]：設定したファン速度とサーバで実行している実際のファン速度が一致しています。 • [保留中（PENDING）]：設定されているファン ポリシーが有効になっていません。この原因として、以下が考えられます。 • サーバの電源がオフになっている • BIOS POST が完了していない • [ファン ポリシーの上書き（FAN POLICY OVERRIDE）]：指定されたファン速度を、サーバーの設定要件によって決定された実際の速度で上書きします。 （注） Cisco UCS C220 M7、C240 M7、C220 M6、C240 M6、UCS C220 M5、C240 M5、C240 SD M5、C125 M5、C480 M5、C480 M5 ML の場合、**[適用されるファン ポリシー（Applied Fan Policy）]** は、サーバーに存在する PCIe カードによって異なります。 Cisco UCS C225 M6 および C245 M6 の場合、**[適用されるファン ポリシー（Applied Fan Policy）]** は、サーバーに存在する PCIe カードまたは特定の CPU タイプによって異なります。
[急速冷却の有効化（Enable Aggressive Cooling）] チェックボックス	急速冷却を有効にするには、このオプションをオンにします。 （注） このオプションは、Cisco UCS C220 M7、C240 M7、C220 M6、C240 M6、C245 M6、および C225 M6 サーバーでのみ使用できます。

ステップ 4 **[Save Changes]**をクリックします。

DIMM のブラックリスト化の設定

DIMM のブラックリスト化

Cisco IMC で、デュアル インライン メモリ モジュール（DIMM）の状態は、SEL イベント レコードに基づいています。BIOS が BIOS ポスト中のメモリ テスト実行時に 16000 のエラー件数を伴う修正不可能なメモリ エラーまたは修正可能なメモリ エラーに遭遇した場合、DIMM は不良と判断されます。不良とマークされた DIMM は機能しないデバイスと見なされます。

DIMM のブラックリスト化を有効にすると、Cisco IMC はメモリ テスト実行メッセージをモニタし、あらゆる時点でDIMM SPD データ内でメモリ エラーに遭遇した DIMM をブラックリストに載せます。これにより、ホストはこれらの DIMM をマップから外すことができます。

DIMM がマップから外されるかまたはブラックリストに追加されるのは、修正不可能なエラーが発生した場合だけです。DIMM がブラックリスト化されると、同じチャネル上にある他の DIMM が無視されるかディセーブルとなり、その DIMM は不良として見なされなくなります。

（注） 16000 修正可能エラーの場合、DIMM がマップから外されることや、ブラックリストに追加されることはありません。

DIMM のブラックリストのイネーブル化

始める前に

- 管理者としてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 [シャーシ（Chassis）] メニューで [インベントリ（Inventory）] をクリックします。

ステップ 3 [Inventory] ペインの [Memory] タブをクリックします。

ステップ 4 [Memory] ペインの [DIMM Black Listing] 領域で、[Enable DIMM Black List] チェックボックスをオンにします。

BIOS の設定

Configuring BIOS Settings

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[コンピューティング（Compute）]メニューをクリックします。

ステップ 2 [コンピューティング（Compute）] メニューで、[BIOS] タブをクリックします。

ステップ 3 [BIOS] タブで、[BIOSの設定（Configure BIOS）] タブをクリックします。

ステップ 4 サーバー モデル別 BIOS パラメータを参照して次のタブを更新します：

- I/O
- サーバ管理
- セキュリティ
- プロセッサ
- メモリ
- 電源/パフォーマンス

（注） 使用可能な BIOS パラメータは、使用しているサーバのモデルによって異なります。

重要 1タブ 個のタブで使用できる BIOS パラメータは、表示しているタブのパラメータだけではなく、すべての利用可能なタブのパラメータに影響を与える可能性があります。

BIOS セットアップの開始

始める前に

- サーバの電源が投入されている。
- このタスクを実行するには、admin権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの [コンピューティング（Compute）] メニューをクリックします。

ステップ 2 **作業ウィンドウで [BIOS]** タブをクリックします。

ステップ 3 [Actions] 領域で [Enter BIOS Setup] をクリックします。

ステップ 4 プロンプトで [OK] をクリックします。
BIOS セットアップの開始が有効になります。再起動時に、サーバは BIOS セットアップを開始します。

BIOS CMOS のクリア

始める前に

- サーバの電源が投入されている。
- このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの [コンピューティング（Compute）] メニューをクリックします。

ステップ 2 **作業ウィンドウで [BIOS]** タブをクリックします。

ステップ 3 **[Actions]**領域の **[Clear BIOS CMOS]** をクリックします。

ステップ 4 **[OK]**をクリックして確定します。
BIOS CMOS がクリアされます。

製造元のカスタム BIOS 設定の復元

始める前に

- サーバーの電源が投入されている。
- このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[コンピューティング（Compute）]メニューをクリックします。
ステップ 2 **[コンピューティング（Compute）]**メニューでサーバを選択します。
ステップ 3 **作業ウィンドウで [BIOS]** タブをクリックします。
ステップ 4 [Actions] 領域で、[Restore Manufacturing Custom Settings] をクリックします。
ステップ 5 サーバをすぐに再起動する場合は、**[はい (Yes)]** をクリックします。
ステップ 6 [OK] をクリックして確定します。

BIOS デフォルトの復元

始める前に

- サーバの電源が投入されている。
- このタスクを実行するには、admin権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[コンピューティング（Compute）]メニューをクリックします。
ステップ 2 **[コンピューティング（Compute）]**メニューでサーバを選択します。
ステップ 3 **作業ウィンドウで [BIOS]** タブをクリックします。
ステップ 4 **[アクション (Actions)]** 領域で、**[デフォルトの復元 (Restore Defaults)]** をクリックします。
ステップ 5 サーバをすぐに再起動する場合は、**[はい (Yes)]** をクリックします。
ステップ 6 [OK] をクリックして確定します。

BIOS プロファイル

Cisco UCS サーバでは、デフォルトのトークン ファイルはすべての S3260 サーバ プラットフォームに使用可能で、グラフィック ユーザ インターフェイス（GUI）、CLIインターフェイス、および XML API インターフェイスを使用して、これらのトークンの値を設定できます。サーバーパフォーマンスを最適化するには、これらのトークン値を特定の組み合わせで設定する必要があります。

BIOS プロファイルを設定することで、正しい組み合わせのトークン値が設定された事前設定トークン ファイルを使用することができます。利用可能な事前設定プロファイルには、仮想

化、高性能、低電力などがあります。シスコの Web サイトから事前設定トークン ファイルのさまざまなオプションをダウンロードし、BMC を介してサーバに適用できます。

ダウンロードしたプロファイルを編集し、トークンの値を変更したり、新しいトークンを追加したりできます。これにより、応答時間なしで、要件に合わせてプロファイルをカスタマイズできます。

BIOS プロファイルのアップロード

リモート サーバの場所またはブラウザ クライアントから BIOS プロファイルをアップロードできます。

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの [コンピューティング（Compute）] メニューをクリックします。

ステップ 2 **作業ウィンドウで [BIOS]** タブをクリックします。

ステップ 3 **[BIOS プロファイルの設定（Configure BIOS Profile）]**タブをクリックします。

ステップ 4 リモート サーバの場所を使用して BIOS プロファイルをアップロードするには、**[BIOS プロファイル（BIOS Profile）]**領域で **[アップロード（Upload）]**ボタンをクリックします。

ステップ 5 [**BIOS プロファイルのアップロード（Upload BIOS Profile）]** ダイアログボックスで、次のフィールドを更新します。

名前	説明
[Upload BIOS Profile from] ドロップダウン リスト	リモート サーバーのタイプ。次のいずれかになります。 • **TFTP** • **FTP** • **SFTP** • **SCP** • **[HTTP]**
[サーバーIP/ホスト名（Server IP/Hostname）] フィールド	BIOSプロファイル情報を有効にするサーバーの IP アドレスまたはホスト名。[Upload BIOS Profile from] ドロップダウン リストの設定によって、フィールド名は異なる場合があります。

名前	説明
[パスおよびファイル名（Path and Filename）] フィールド	リモート サーバー上の BIOS プロファイルのパスおよびファイル名。
[ユーザ名（Username）] フィールド	リモート サーバのユーザ名。
[パスワード（Password）]フィールド	リモート サーバのパスワード。
[アップロード（Upload）] ボタン	選択したBIOSプロファイルをアップロードします。 （注） このアクションを実行中にリモート サーバのタイプとして SCP または SFTP を選択した場合、ポップアップ ウィンドウが表示され、そこに *[*サーバ（*RSA*）鍵フィンガープリントは *<server_finger_print _ID>* です。続行しますか*?*（*Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?*）*]* というメッセージが表示されます。サーバフィンガープリントの信頼度に応じて、[Yes] または [No] をクリックします。 フィンガープリントはホストの公開キーをベースにしており、接続先ホストの特定や確認に利用できます。
[Cancel]ボタン	サーバに保管されているファームウェア バージョンには変更を加えることなく、ウィザードを閉じます。

ステップ 6 ブラウザ クライアントを使用して BIOS プロファイルをアップロードするには、**[BIOS プロファイル（BIOS Profile）]** 領域で **[アップロード（Upload）]** ボタンをクリックします。

ステップ 7 **[BIOS プロファイルのアップロード（Upload BIOS Profile）]** ダイアログボックスで、次のフィールドを更新します。

名前	説明
[File] フィールド	アップロードする BIOS プロファイル。

名前	説明
[Browse] ボタン	ダイアログボックスが表示され、そこで、該当するファイルにナビゲートすることができます。

次のタスク

BIOS プロファイルをアクティブにします。

BIOS プロファイルのアクティブ化

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[コンピューティング（Compute）]メニューをクリックします。

ステップ 2 **作業ウィンドウで [BIOS]** タブをクリックします。

ステップ 3 **[BIOS プロファイルの設定（Configure BIOS Profile）]** タブをクリックします。

ステップ 4 **[BIOS プロファイル（BIOS Profile）]** 領域から BIOS プロファイルを選択し、**[アクティブ化（Activate）]**をクリックします。

ステップ 5 プロンプトで **[はい（Yes）]**をクリックし、BIOS プロファイルをアクティブにします。

BIOS プロファイルの削除

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[コンピューティング（Compute）]メニューをクリックします。

ステップ 2 **[コンピューティング（Compute）]**メニューでサーバを選択します。

ステップ 3 **作業ウィンドウで [BIOS]** タブをクリックします。

ステップ 4 [BIOS Profile] 領域から BIOS プロファイルを選択し、[Delete] をクリックします。

ステップ 5 プロンプトで **[OK]**をクリックし、BIOS プロファイルを削除します。

BIOS プロファイルのバックアップ

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[コンピューティング（Compute）]メニューをクリックします。

ステップ 2 **[コンピューティング（Compute）]**メニューでサーバを選択します。

ステップ 3 **作業ウィンドウで [BIOS]** タブをクリックします。

ステップ 4 [BIOS Profile] 領域から BIOS プロファイルを選択し、[Take Backup] をクリックします。

ステップ 5 プロンプトで**[OK]**をクリックし、BIOS プロファイルのバックアップを作成します。

次のタスク

BIOS プロファイルをアクティブにします。

BIOS プロファイルの詳細の表示

始める前に

このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの[コンピューティング（Compute）]メニューをクリックします。

ステップ 2 **[コンピューティング（Compute）]**メニューでサーバを選択します。

ステップ 3 **作業ウィンドウで [BIOS]** タブをクリックします。

ステップ 4 [BIOS Profile] 領域から BIOS プロファイルを選択し、[Details] をクリックします。

ステップ 5 **[BIOS プロファイルの詳細（BIOS Profile Details）]**ウィンドウで、次の情報を確認します。

名前	説明
[トークン名（Token Name）] カラム	BIOS プロファイルのトークン名が表示されます。
[表示名（Display Name）] カラム	BIOS プロファイルのユーザ名が表示されます。
[プロファイル値（Profile Value）] カラム	アップロードされたファイルに設定された値が表示されます。
[実際の値（Actual Value）] カラム	アクティブな BIOS 設定の値が表示されます。

セキュアブート証明書の管理

4.2 (2a) リリース以降、Cisco IMC では、設定されたセキュア HTTP ブート デバイス用に最大 10 個の証明書をアップロードできます。構成された特定のブート デバイスの新しい証明書を削除してアップロードすることもできます。Cisco IMC では、最大 10 個のルート CA 証明書をアップロードできます。

セキュアブート証明書の詳細の表示

アップロード済みのセキュア ブート証明書の詳細を表示できます。

始める前に

このタスクを実行するには、admin 権限を持つユーザーとして admin としてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [コンピューティング（Compute）] メニューをクリックします。

ステップ 2 **作業ウィンドウで [BIOS]** タブをクリックします。

ステップ 3 **[セキュアブート証明書の管理（Secure Boot Certificate Management）]**タブをクリックします。

ステップ 4 証明書の表から、表示したい証明書を選択します。

ステップ 5 テーブルの上にある **[セキュア ブート証明書の表示（View Secure Boot Certificate）]** アイコンをクリックします。

ステップ 6 **[セキュア ブート証明書の表示（View Secure Boot Certificate）]** ダイアログ ボックスが表示されます。

以下の情報を確認できます。

表 *1 :* [一般（*General*）] 領域

フィールド	説明
[証明書識別子（Certificate ID）] フィールド	Cisco IMC によって割り当てられた証明書識別子を表示します。
[Serial Number] フィールド	サーバーのシリアル番号。
[Valid From] フィールド	証明書の有効期間の開始日
[Valid To] フィールド	証明書の失効日。

表 *2 :* サブジェクト エリア

フィールド	説明
[Country Code] フィールド	証明書の国コード。
[Locality] フィールド	証明書の地域。
[State Name] フィールド	証明書の状態。
[組織名（Organization Name）] フィールド	証明書の組織。
[Organization Unit] フィールド	証明書の組織単位。
[Common Name] フィールド	証明書名。

表 *3 :* 発行者エリア

フィールド	説明
[Country Code] フィールド	発行者の国コード。
[Locality] フィールド	発行者の地域。
[State Name] フィールド	発行者の状態。
[組織名（Organization Name）] フィールド	発行者の組織。
[Organization Unit] フィールド	発行者の組織単位。
[Common Name] フィールド	発行者名。

セキュア ブート証明書のアップロード

ブート証明書は、リモート サーバーの場所またはローカルの場所からアップロードできます。

始める前に

- このタスクを実行するには、admin 権限を持つユーザーとして admin としてログインする必要があります。
- ローカルアップロードを使用してアップロードする場合は、証明書ファイルがローカルでアクセス可能なファイル システムに存在することを確認してください。
- 生成された証明書のタイプが [Server] であることを確認します。
- 次の証明書形式がサポートされています。
  - .crt
  - .cer
  - .pem

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [コンピューティング（Compute）] メニューをクリックします。

ステップ 2 作業ウィンドウで **[BIOS]** タブをクリックします。

ステップ 3 **[セキュアブート証明書の管理（Secure Boot Certificate Management）]**タブをクリックします。

ステップ 4 起動証明書をアップロードするには、アップロード ボタン（+）をクリックします。

ステップ 5 次のいずれかの方法を使用して、証明書をアップロードできます：

- 証明書の貼り付けテキスト フィールドに証明書を直接貼り付けます
- ローカル ロケーションからアップロード
- リモートロケーションからアップロード

[セキュア ブート証明書の追加（Add Secure Boot Certificate）] ダイアログ ボックスで、証明書をアップロードする方法に従ってフィールドを更新します：

表 *4:* セキュアブート証明書の追加

フィールド	説明
[セキュア ブート証明書を貼り付け（Paste Secure Boot Certificate）] ラジオ ボタン	署名付き証明書の内容全体をコピーして、証明書の内容を貼り付けテキスト フィールドに貼り付けることができます。 （注） アップロードの前に、証明書に署名が付されていることを確認します。
[ローカルラジオ（Upload from local）] ボタンからアップロード	追加する認証局証明書ファイルの場所を参照してナビゲートできます。

フィールド	説明
[リモート ロケーションからアップロード（Download from remote location）] ラジオ ボタン	リモートロケーションの証明書を選択してアップロードできます。次の詳細を入力します。 • からセキュアブート証明書をアップロード— • TFTP サーバ • FTP サーバ • SFTP サーバ • SCP サーバ • HTTP サーバ • **[サーバー IP/ホスト名（Server IP/Hostname）]**— 証明書ファイルの保管先とするサーバーの IP アドレスまたはホスト名。ドロップダウン リストの証明書アップロードの設定に応じて、フィールドの名前が異なる場合があります。 • **[パスおよびファイル名（Path and Filename）]**：リモート サーバーにファイルをアップロードする際に Cisco IMC が使用する必要があるパスおよびファイル名。 • **[ユーザ名（Username）]**— リモート サーバーにログインするためにシステムが使用するユーザー名。プロトコルが TFTP または HTTP の場合、このフィールドは適用されません。 • **[パスワード（Password）]**—リモート サーバーのユーザー名のパスワード。プロトコルが TFTP または HTTP の場合、このフィールドは適用されません。
セキュアブート証明書ボタンのアップロード	証明書をサーバーにアップロードできるようにします。

セキュアブート証明書の削除

Cisco IMC にすでにアップロードされているブート証明書を削除できます。

始める前に

このタスクを実行するには、admin 権限を持つユーザーとして admin としてログインする必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [コンピューティング（Compute）] メニューをクリックします。

ステップ 2 **作業ウィンドウで [BIOS]** タブをクリックします。

ステップ 3 **[セキュアブート証明書の管理（Secure Boot Certificate Management）]**タブをクリックします。

ステップ 4 証明書の表から、削除したい証明書を選択します。

ステップ 5 テーブルの上にある **[セキュア ブート証明書の削除（Delete Secure Boot Certificate）]** アイコンをクリックします。

ステップ 6 確認のために [はい（Yes）] をクリックします。

前面パネルの動的温度しきい値の設定

前面パネルの動的温度しきい値オプションを使用すると、前面パネルの温度センサーの重要な上限しきい値を設定できます。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）] メニューをクリックします。

ステップ 2 [シャーシ（Chassis）] メニューの [センサー（Sensors）] をクリックします。

ステップ 3 [センサー（Sensors）] ペインの [温度（Temperature）] タブをクリックします。

ステップ 4 [前面パネルの動的温度しきい値（Dynamic Front Panel Temperature Threshold）] 領域を展開し、[クリティカル（Critical）] フィールドで前面パネルの温度センサーの重要な上限しきい値を入力します。8 ～ 50 の値を入力できます。

ステップ 5 **[Save Changes]**をクリックします。

永続メモリ モジュール

Cisco UCS C シリーズ リリース 4.0(4) は、Intel® Optane™ Data Center 永続メモリ モジュール (第二世代インテル® Xeon® Scalable プロセッサに基づく UCM M5 サーバ上) のサポートを導入します。永続メモリ モジュールは、第二世代インテル® Xeon® Scalable プロセッサでのみ使用できます。

永続メモリ モジュールは、メモリの低遅延とストレージの永続化を実現する不揮発性メモリ モジュールです。永続メモリ モジュールに保存されているデータは、他のストレージ デバイスに比べてすぐにアクセスでき、電源サイクルで保持されます。

永続メモリ モジュールの設定の詳細については、『Cisco UCS: Intel® Optane™ Data Center 永続メモリモジュールの設定と管理』を参照してください。

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。