



Cisco ベースボード管理コントローラ GUI 構成ガイド、リリース 2.0

最終更新：2026 年 1 月 6 日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>



目次

はじめに :

はじめに	ix
対象読者	ix
表記法	ix

第 1 章

はじめに	1
の概要 Cisco UCS C845A M8 ラック サーバー	1
サーバソフトウェアの概要	2
サーバソフトウェアの要件	2
ログインします。Cisco BMC 2.0	3
ナビゲーションとメニュー	3
ダッシュボード	7
サーバポート	9

第 2 章

サーバ OS のインストール	11
OS のインストール方法	11
仮想 KVM コンソール	11
KVM コンソールを使用した OS のインストール	12

第 3 章

サーバの管理	15
Intersight Infrastructure Service ライセンス	15
サーバ サマリの表示	16
インベントリの表示	18
センサー ステータスの表示	25
タイムゾーンの構成	25

サーバーのブート	26
UEFI セキュア ブートの概要	26
ブート順の構成	27
サーバーの実際のブート順の表示	28
UEFI セキュア ブートの有効化または無効化	28
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	28
BIOS トークン	29
I/O BIOS パラメータの構成	29
サーバ管理 BIOS パラメータの構成	31
セキュリティ BIOS パラメータの構成	35
メモリ BIOS パラメータの構成	37
プロセッサの BIOS パラメータの構成	44
電源とパフォーマンスの BIOS パラメータの構成	47
電力ポリシーの設定	50
電力制限	50
CPU 電力制限の有効化	50
CPU 電力構成の表示	50
電力復元ポリシーの構成	51

第 4 章

ユーザー アカウントの管理	53
ユーザ管理	53
ユーザーの追加	53
ユーザの編集	54
ユーザーの有効化または無効化	56
アカウント ポリシー設定を管理	56
ユーザの削除	57
パスワード設定の管理	57
LDAP 設定	59
LDAP 認証のイネーブル化	59
ロール グループの追加	60
Active Directory	61

	Active Directory サーバーの構成	61
	ユーザ セッション	62
	ユーザ セッションの表示	62
	セッションの切断	63

第 5 章	リモート プレゼンスの管理	65
	仮想メディアの設定	65
	仮想メディアの構成	65
	仮想 KVM コンソール	66
	KVM コンソールの起動	69
	仮想 KVM の設定	69
	仮想 KVM の無効化	70

第 6 章	ネットワーク関連の設定	71
	ネットワーク設定内の構成内の Cisco BMC 2.0	71
	ネットワーク設定の表示または構成	71
	IPv4 アドレスの表示または追加	73
	IPv6 アドレスの表示または追加	74
	静的 DNS IP アドレスの表示、追加、または削除	75
	ドメイン名の表示、追加、または削除	75
	Network Time Protocol の設定	76
	Network Time Protocol 設定の指定	76

第 7 章	ストレージ設定の管理	79
	コントローラの管理	79
	変更管理チケット情報の表示	79
	NVMe 物理ドライブ情報の表示	80
	仮想ドライブ情報の表示	82
	NVMe ドライブの管理	83
	NVME サブシステム情報の表示	83
	NVME のバイタル製品データ情報の表示	87

NVMe ドライブ情報の表示	88
NVMe ドライブ ロケータ LED の有効化または無効化	90

第 8 章	証明書セキュリティの管理	91
	証明書の詳細の表示	91
	新しい証明書の追加	92
	証明書を置き換えています	93
	証明書を削除する	93
	証明書署名要求を生成する	93

第 9 章	障害とログの管理	97
	システム イベント ログ	97
	システム イベント ログの表示	97
	イベント ログのエクスポート	98
	システム イベント ログの削除	99
	POST ログ	99
	POST コードログの表示	99
	POST コード ログのエクスポート	100
	テクニカル サポート ログ	100
	テクニカル サポート ログのエクスポート	100
	テクニカル サポート ログのダウンロード	102

第 10 章	ユーティリティとイベント管理の構成	103
	イベント管理設定の構成	103
	実践中 Cisco BMC 2.0 工場出荷時の状態へのリセット	104
	リブート Cisco BMC 2.0	104

第 11 章	ファームウェアの管理	105
	ファームウェア管理の概要	105
	ファームウェア コンポーネントの表示	105
	BMC ファームウェアのアップデート	106

第 12 章	コミュニケーション サービスの設定	107
	TLS の有効化または無効化	107
	IPMI の設定	108
	IPMI (アウトオブバンド) の構成	108
	SSH の設定	108
	SOL 不揮発性ビットレートの構成	109
	Web セッション タイムアウトの構成	109
	OpenSSL FIPS モードの有効化または無効化	110
	Web ポート値の構成	110
	電子メール アラートを受信するための SMTP サーバの構成	111
	電子メール受信者の追加	112

第 13 章	Device Connector の管理	113
	Intersight 管理モード	113
	デバイス コネクタを有効化または無効化	114
	プロキシ設定	114
	証明書のインポートまたは、表示	115
	アプライアンス接続のチェック	116



はじめに

この前書きは、次の項で構成されています。

- [対象読者](#) (ix ページ)
- [表記法](#) (ix ページ)

対象読者

このガイドは、次の1つ以上に責任を持つ、専門知識を備えたデータセンター管理者を主な対象にしています。

- サーバ管理
- ストレージ管理
- ネットワーク管理
- ネットワーク セキュリティ

表記法

テキストのタイプ	説明
GUI 要素	タブの見出し、領域名、フィールドのラベルのような GUI 要素は、 このフォント のように表示されます。 ウィンドウ、ダイアログボックス、ウィザードのタイトルのようなメインタイトルは、 このフォント のように表示されます。
マニュアルのタイトル	マニュアルのタイトルは、 このフォント のように表示されます。
TUI 要素	テキストベースのユーザーインターフェイスでは、システムによって表示されるテキストは、 このフォント のように表示されます。

テキストのタイプ	説明
システム出力	システムが表示するターミナルセッションおよび情報は、このフォントのように表示されます。
CLI コマンド	CLI コマンドのキーワードは、 this font のように表示されます。 CLI コマンド内の変数は、このフォントのように表示されます。
[]	角カッコの中の要素は、省略可能です。
{x y z}	どれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x y z]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
<>	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!, #	コードの先頭に感嘆符 (!) またはポンド記号 (#) がある場合には、コメント行であることを示します。



(注) 意味は、「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。



ヒント 意味は、「問題解決に役立つ情報」です。ヒントには、トラブルシューティングや操作方法ではなく、ワンポイントアドバイスと同様に知っておくと役立つ情報が記述される場合もあります。



ワンポイントアドバイス

意味は、「時間を節約する方法」です。ここに紹介している方法で作業を行うと、時間を短縮できます。



注意 意味は、「要注意」です。機器の損傷またはデータ損失を予防するための注意事項が記述されています。



警告 安全上の重要事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。各警告の最後に記載されているステートメント番号を基に、装置に付属の安全についての警告を参照してください。

これらの注意事項を保管しておいてください。



第 1 章

はじめに

- [の概要 Cisco UCS C845A M8 ラック サーバー \(1 ページ\)](#)
- [サーバ ソフトウェアの概要 \(2 ページ\)](#)
- [サーバ ソフトウェアの要件 \(2 ページ\)](#)
- [ログインします。 Cisco BMC 2.0 \(3 ページ\)](#)
- [ナビゲーションとメニュー \(3 ページ\)](#)
- [ダッシュボード \(7 ページ\)](#)
- [サーバポート \(9 ページ\)](#)

の概要 Cisco UCS C845A M8 ラック サーバー

Cisco UCS C845A M8 ラック サーバー は、アクセラレーション コンピューティングのための NVIDIA MGX リファレンス デザインに基づいた、拡張性、柔軟性、およびカスタマイズ可能な AI システムです。2 ~ 8 個の NVIDIA PCIe GPU と NVIDIA AI Enterprise ソフトウェアをサポートしているため、Generative AI の微調整と推論を含む幅広い AI ワークロードで高いパフォーマンスを提供します。

Cisco UCS C845A M8 サーバは、2 ~ 8 個の GPU で構成できます。構成に応じて、PCIe ベースの NVIDIA H100 NVL、H200 NVL、L40S、RTX6000 Pro、または AMD GPU MI210 から選択できます。MGX 設計の洗練により、他の次世代 NVIDIA GPU も、これらの GPU が利用可能になると、この同じプラットフォームに導入される予定です。

AI ワークロード向けに特別に設計された AMD の新しいハイエンド Turin (第 5 世代) CPU を搭載したコンピューティング ノードにより、Cisco UCS C845A M8 AI サーバー内のボトルネックを回避するために必要な CPU または GPU パフォーマンスに妥協のないソリューションが提供されます。もう 1 つの利点は、NVIDIA ConnectX-7 NIC および/または NVIDIA BlueField-3 DPU を使用してサーバーを構成して、サーバーとの間のデータ トラフィックを処理できることです。

NVIDIA H100 NVL または H200 NVL GPU を搭載したシステムには、NVIDIA AI Enterprise の 5 年間ライセンスが付属しています。NVIDIA AI Enterprise は、AI エージェント、生成 AI、コンピュータ ビジョン、音声 AI などを含んでいます。使いやすいマイクロサービスにより、エンタープライズレベルのセキュリティ、サポート、および安定性によってモデルのパフォーマンスが最適化され、AI で事業を展開する企業のプロトタイプから実稼働へのスムーズな移行

が保証されます。詳細については、次を参照してください。 [Cisco UCS C845A M8 ラック サーバ](#)を参照してください。

Cisco UCS C845A M8 Cisco ベースボード管理コントローラ 2.0 REST API ガイド、リリース 2.0 (Cisco BMC 2.0) ファームウェアと共に出荷されるサーバ。Cisco BMC 2.0 は、マザーボードに組み込まれている独立した管理モジュールです。専用の ARM ベースのプロセッサが、メインサーバ CPU とは別に、ファームウェアを Cisco BMC 2.0 実行します。システムにはファームウェアの実行バージョンを組み込んで Cisco BMC 2.0 出荷します。ファームウェアは更新 Cisco BMC 2.0 ですが、初期インストールは必要ではありません。

Cisco UCS C シリーズ ラック サーバーは、Windows、Linux、Oracle などのオペレーティングシステムをサポートします。デバイスでサポートされるオペレーティングシステムの詳細については、以下を参照してください。 [UCS ハードウェアとソフトウェアの互換性](#)を参照してください。Cisco BMC 2.0 を使用して、KVM コンソールおよび vMedia を使ってサーバに OS をインストールできます。

サーバソフトウェアの概要

Cisco ベースボード管理コントローラ 2.0 REST API ガイド、リリース 2.0 (Cisco BMC 2.0) は、Cisco UCS C845A M8 サーバの管理サービスです。Cisco BMC 2.0 はサーバ内で動作します。



- (注) Cisco BMC 2.0 管理サービスは、サーバがスタンドアロン モードで動作している場合にだけ使用されます。サーバが UCS システムに統合される場合、Cisco Intersight を使用して管理する必要があります。 [\[Cisco Intersight ヘルプ センター \(Cisco Intersight Help Center\)\]](#) を確認して、サーバの管理方法について詳細をご覧ください。

Web ベースの GUI、SSH ベースの CLI、または REST API を使用して、サーバにアクセスし、サーバを構成、管理、モニタできます。各インターフェイスは異なる機能を提供し、各インターフェイスでサポートされているタスクについては、それぞれのコンフィギュレーションガイドで説明されています。次の操作を実行することはできません。

- Cisco BMC 2.0 GUI を使用して、Cisco BMC 2.0 CLI を呼び出します。
- CLI で呼び出したコマンドを Cisco BMC 2.0 GUI に Cisco BMC 2.0 生成します。
- GUI から Cisco BMC 2.0 CLI 出力を Cisco BMC 2.0 生成します。

サーバソフトウェアの要件

ブラウザの最新の仕様については、次を参照してください。 [Cisco ベースボード管理コントローラ 2.0 リリース ノート、リリース 2.0](#)。

ログインします。 Cisco BMC 2.0

手順

ステップ 1 Web ブラウザで、への Web リンクを入力または選択します。 Cisco BMC 2.0。

ステップ 2 セキュリティ ダイアログボックスが表示された場合は、次の操作を実行します。

- (任意) チェックボックスをオンにして、Cisco からのすべてのコンテンツを受け入れます。
- 次をクリックします **はい** をクリックして、証明書を受け入れ、続行します。

ステップ 3 ログイン ウィンドウで、ユーザ名とパスワードを入力します。

未設定のシステムに初めてログインする場合は、ユーザ名に **admin**、パスワードに **password** を使用します。

Web UI に初めてログインする際、次のようになります。

- Web UI または CLI でデフォルトの管理者クレデンシャルを変更するまでは、操作を実行 Cisco BMC 2.0 できません。
- パスワードの変更ポップアップウィンドウを閉じたりキャンセルしたりすることはできません。UI をタブで開くか、ブラウザ ページを更新すると、ポップアップウィンドウが引き続き表示されます。このポップアップウィンドウは、初期設定へのリセット後にログインすると表示されます。
- 新しいパスワードとして 'password' の語を選択することはできません。スクリプトを実行する際にこのことが問題になる場合は、ユーザ管理オプションにログインし直すことによって、それをパスワードに変更することができますが、これは完全に自己責任において実行するようにしてください。シスコでは推奨していません。

ステップ 4 登録手続きを開始するには、**ログイン**。

ナビゲーションとメニュー

ログイン時 Cisco BMC 2.0 に [**ダッシュボード (Dashboard)**] ページに移動します。次のオプションが使用可能であることがわかります：

メニューバー

上部のメニューバーには、次のオプションがあります：

表 1:

名前	説明
正常性	システム ヘルスの表示を可能にします。

名前	説明
ホストの電源	暗号ホスト キー操作を実行できます。
KVM の起動	KVM ウィンドウを起動できます。
更新	BMC センサーの値を更新できます。
BMC のリブート	BMC をリブートできます。
ログインするユーザーの名前	現在ログインしているユーザーの名前を表示します。 クリックして、Cisco BMC 2.0 の [CIMC ホスト名 (CIMC Host Name)] および [ログアウト (logout)] ボタンを表示します。

ナビゲーション

Cisco BMC 2.0 GUI の左側のナビゲーション ウィンドウは、次のドロップダウン リストで構成されます。

Dashboard

[ダッシュボード (Dashboard)] アプリには次の情報が表示されます。

- [サーバのプロパティ (Server Properties)] : 製品名、シリアル番号などのサーバの詳細を表示します。また、BIOS の概要、ブート順序、およびアクションを表示できます。
- Cisco BMC 2.0 [情報 (Information)] : 表示 Cisco BMC 2.0 [CIMC 情報 (CIMC Information)] : IP アドレス、MAC アドレスなどの Cisco IMC 情報が表示されます。また、タイムゾーンを表示および更新できます。
- [シャーシステータス (Chassis Status)] : サーバコンポーネント全体のステータスを表示します。
 - [電源ステータス (Power Status)] : サーバの電源がオンかオフかを示します。
 - [POST 完了ステータス (Post Completed Status)] : 電源投入時自己診断テスト (POST) プロセスが完了したかどうかを示します。
 - 全体のサーバステータス : サーバの一般的な動作ステータスを表します。
 - [温度 (Temperature)] : サーバコンポーネントの温度ステータスを表示します。
 - [全体 DIMM ステータス (Overall DIMM Status)] : メモリ モジュールの正常性ステータスを示します。
 - [電源 (Power Supplies)] : 電源装置の動作ステータスを反映します。
 - [ファン (Fans)] : サーバの冷却ファンのステータスを示します。

- [ロケータ LED (Locator LED)] : サーバのロケータ ライトがアクティブになっているかどうかを示します。
- [ストレージ全体のステータス (Overall Storage Status)] : ストレージデバイスの正常性とステータスを表します。
- [システム識別 LED (System Identify LED)] : システム識別 LED が点灯または消灯しているかどうかを示します。

システム

[システム (System)] アプリには、次のタブが含まれています。

- [インベントリ (Inventory)] : CPU、メモリ、PCI アダプタ、電源装置、Cisco VIC アダプタ、ネットワーク アダプタ、ストレージ、SAS エクспанダ、および TPM。
- [センサー (Sensors)] : 電源装置、ファン、温度、電圧、電流、LED、およびストレージ。
- [電源管理 (Power Management)] : 電力制限の構成と電源モニタリング。
- [ログ (Logs)] : 障害サマリ、障害履歴、システム イベント ログ Cisco BMC 2.0 ログ、ロギング制御

コンピューティング

[コンピューティング アプリ (ComputeApp)] には、サーバに関する次の情報が含まれています。

- [BIOS] : インストールされている BIOS ファームウェア バージョンと BIOS プロファイル構成、サーバのブート順序設定、I/O、サーバ管理、セキュリティ、プロセッサ、メモリ、電源、またはパフォーマンス。
 - トークン
 - ブート順序
 - プロファイル
 - セキュアブート証明書の管理
- [リモート管理 (Remote Management)] : LAN 設定上の KVM、仮想メディア、およびシリアル。
- [電源復元ポリシー (Power restore policy)] : 電源障害後のシステムの動作を構成できます。[常にオン (Always On)]、[常にオフ (Always Off)]、[最後の状態 (Last State)] などのオプションがあります。

ストレージ

[ストレージ アプリ (Storage App)] には、次のメニューが含まれています。

- コントローラ
 - [コントローラ情報 (Controller Info)] : RAID コントローラに関する一般的な情報と設定情報。
 - [物理ドライブ情報 (Physical Drive Info)] : 一般的な物理ドライブと対応する RAID 情報。
 - [仮想ドライブ情報 (Virtual Drive Info)] : 一般的な仮想ドライブと対応する RAID 情報。
- [NVMe情報 (NVMe Information)] : モデル、シリアル番号、製品番号、製造元、およびその他の関連情報を含む、インストール済みの NVMe ソリッドステートドライブに関する詳細が表示されます。

管理

[管理 アプリ (Administration App)] には、次のメニューが含まれています。

- [ユーザー管理 (User Management)] : ローカルユーザー管理、LDAP、セッション管理、および TACACS+。
- [ネットワーキング (Networking)] : ネットワークプロパティおよびネットワーク設定。
- [通信サービス (Communication Services)] : HTTP、SSH、XML API、Redfish のプロパティ、IPMI over LAN のプロパティ、[SNMP] タブには [SNMP のプロパティ (SNMP Properties)]、[ユーザー設定 (User Settings)]、[トラップ接続先 (Trap Destinations)]、[メールアラート (Mail Alert)] タブには SMTP のプロパティと SMTP 受信者。
 - [通信サービス (Communication Services)] : HTTP プロパティ、SSH プロパティ、XML API プロパティ、Redfish プロパティ、Serial over LAN、TLS 構成、および IPMI over LAN プロパティ
 - [SNMP] : SNMP のプロパティ、ユーザー設定、およびトラップ宛先
 - [メールアラート (Mail Alert)] : SMTP プロパティと SMTP 受信者
- [セキュリティ管理 (Security Management)] : 証明書管理、セキュリティキー管理、セキュリティ構成、MCTP SPDM。
- [イベント管理 (Event Management)] : プラットフォームイベントフィルタの有効化/無効化およびイベントフィルタのリセット
- [ファームウェア管理 (Firmware Management)] : Cisco BMC 2.0 および BIOS ファームウェア情報と管理。
- [ユーティリティ (Utilities)] : 最終テクニカルサポートデータのエクスポート、Cisco BMC 2.0 最終リセット、Cisco BMC 2.0 構成のインポート/エクスポート、インベントリデータ、VIC アダプタのインポート/エクスポート、工場出荷時のデフォルト状態、前面パネル USB。

- [デバイス コネクタ (Device Connector)] : Cisco Intersight 管理およびネットワーク設定。

ダッシュボード

GUI にログインした Cisco BMC 2.0 後、**ダッシュボード** ページで設定しなければならない場合があります。このページから、重要な機能や情報にすばやくアクセスできます。次に、[概要 (Overview)] ページの主要なプロパティとセクションを示します。

システム情報 (System Information)

表 2: サーバ プロパティ

名前	説明
製品名 (Product Name) field	このフィールドには、サーバの製品名が表示されます。
シリアル番号 (Serial Number) field	このフィールドには、サーバーに割り当てられた一意のシリアル番号が含まれます。
UUID field	このフィールドには、サーバの UUID が含まれています。
BIOS Version field	このフィールドには、実行中の BIOS バージョンが表示されます。
説明 フィールド	このフィールドには、システムの説明が表示されます。
Asset Tag field	このフィールドには、サーバーのアセット タグが含まれています。

表 3: Cisco BMC 2.0 情報

名前	説明
ホストネーム (Hostname) field	このフィールドには、サーバのホスト名が表示されます。
IP アドレス (IP Address) field	このフィールドには、サーバーの IP アドレスが表示されます。
MAC アドレス field	このフィールドは、サーバの MAC アドレスを示します。
ファームウェアバージョン (Firmware Version) field	このフィールドは、サーバのファームウェアバージョンを示します。

名前	説明
[現在の時刻 (ユニバーサル) (Current Time (Universal))] field	このフィールドには、現在の万国標準時が表示されます。
Timezone field	このフィールドは、サーバのタイムゾーン設定を示します。
タイムゾーンを選択 リンク	タイムゾーンを変更できます。「タイムゾーントピックのプレースホルダ」を参照してください。

[Status Information]

表 4: シャーシステータス

オプション	説明
Power Status	サーバの電源がオンかオフかを示します。
完了後のステータス	電源投入時自己診断テスト (POST) プロセスが完了しているかどうかを示します。
サーバ全体のステータス	サーバの一般的な動作ステータスを表します。
温度	サーバ コンポーネントの温度ステータスを表します。
DIMM全体のステータス	メモリ モジュールの正常性ステータスを示します。
電源モジュール	電源ユニットの動作ステータスを反映します。
ファン	サーバの冷却ファンのステータスを表示します。
ロケータ LED	サーバのロケータ ライトがアクティブになっているかどうかを示します。
ストレージ全体のステータス	ストレージ デバイスの正常性とステータスを表示します。

表 5: インベントリと LED

名前	説明
システム識別LED トグル ボタン	このフィールドには、システム識別 LED のステータスが表示されます。この LED は、システムを物理的に識別するためにオンまたはオフに切り替えることができます。

サーバポート

次に示すのは、サーバポートとそのデフォルトのポート番号のリストです。

表 6: サーバポート

ポート名	ポート番号
LDAP Port 1	389
LDAP Port 2	389
LDAP Port 3	389
LDAP Port 4	3268
LDAP Port 5	3268
LDAP Port 6	3268
SSHポート	22
[HTTP ポート (HTTP Port)]	80
HTTPS ポート	443
SMTP ポート (SMTP Port)	25
KVM ポート	2068
Intersight 管理ポート	8889
Intersight クラウド ポート	8888
SOL SSH ポート	2400
SNMPポート	161
SNMP トラップ	162
外部Syslog	514



第 2 章

サーバ OS のインストール

- [OS のインストール方法 \(11 ページ\)](#)
- [仮想 KVM コンソール \(11 ページ\)](#)

OS のインストール方法

Cisco UCS C845A M8 ラック サーバー いくつかのオペレーティング システムをサポートします。インストールされている OS に関係なく、次のいずれかのツールを使用してサーバにインストールできます。

- KVM コンソール

Cisco UCS Server Configuration Utility の詳細については、以下を参照してください。 [Cisco UCS 構成ユーティリティ クイック スタート ガイド](#)。

仮想 KVM コンソール

vKVM コンソールは、サーバへのキーボード、ビデオ、Cisco BMC 2.0 マウス(KVM)の直接接続をエミュレートする GUI からアクセス可能なインターフェイスです。vKVM コンソールを使用すると、リモートの場所からサーバに接続できます。

Cisco KVM コンソールを使用する主な利点は次のとおりです。

- Cisco KVM コンソールは KVM、SOL、および vMedia への接続を提供しますが、Avocent KVM は KVM および vMedia への接続のみを提供します。
- KVM コンソールでは、vMedia 接続が KVM 起動マネージャで確立され、すべてのユーザーが使用できます。
- KVM コンソールには、ゲストからホストにテキストを貼り付ける際に、サポートされていない文字の高度な文字置換オプションが用意されています。
- KVM コンソールには、以下に vMedia マッピングを保存する機能があります。Cisco BMC 2.0。

- 新しい Web GUI では、別のウィンドウを開く必要なく、GUI 自体の中で vKVM コンソールを操作できます。

サーバに物理的に接続された CD/DVD ドライブまたはフロッピー ドライブを使用する代わりに、vKVM コンソールは仮想メディアを使用します。これは、仮想 CD/DVD ドライブまたはフロッピー ドライブにマップされる実際のディスク ドライブまたはディスク イメージファイルです。次のいずれでも仮想ドライブにマップできます。

- コンピュータ上の CD/DVD またはフロッピー ドライブ
- コンピュータ上のディスク イメージファイル (ISO または IMG ファイル)
- コンピュータ上の USB フラッシュ ドライブ
- ネットワーク上の CD/DVD またはフロッピー ドライブ
- ネットワーク上のディスク イメージファイル (ISO または IMG ファイル)
- ネットワーク上の USB フラッシュ ドライブ

vKVM コンソールを使用してサーバに OS をインストールできます。

KVM コンソールを使用した OS のインストール

始める前に

- OS インストール イメージファイルを見つけます。
- OS をインストールするには、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 OS インストールディスクを CD/DVD ドライブにロードするか、ディスク イメージファイルをコンピュータにコピーします。

ステップ 2 メニューから、以下をクリックします。 **KVM の起動** アイコンをクリックします。

KVM セッション ウィンドウが、ブラウザの設定に応じて新しいタブまたはウィンドウとして開きます。

ステップ 3 KVM コンソールで、左側のナビゲーションから **[仮想メディア (Virtual Media)] > [マップイメージ (Map image)]** または **[外部イメージのマッピング (Map external image)]**

ステップ 4 サーバをリブートし、ブート デバイスとして仮想 CD/DVD ドライブを選択します。

サーバを再起動すると、仮想 CD/DVD ドライブからインストールプロセスが開始します。残りのインストールプロセスについては、インストールしている OS のインストールガイドを参照してください。

次のタスク

OS のインストールが完了したら、LAN のブート順を元の設定にリセットします。ソフトウェアの相互運用性とドライバの互換性を含め、常に OS ベンダ推奨の設定に従うようにします。ドライバの推奨事項とインストールについて詳しくは、こちらの「[Cisco UCS ハードウェア互換性マトリクス](#) :」に従ってください。。



第 3 章

サーバーの管理

- [Intersight Infrastructure Service ライセンス \(15 ページ\)](#)
- [サーバー サマリの表示 \(16 ページ\)](#)
- [インベントリの表示 \(18 ページ\)](#)
- [センサー ステータスの表示 \(25 ページ\)](#)
- [タイム ゾーンの構成 \(25 ページ\)](#)
- [サーバーのブート \(26 ページ\)](#)
- [BIOSトークン \(29 ページ\)](#)
- [電力ポリシーの設定 \(50 ページ\)](#)

Intersight Infrastructure Service ライセンス

Cisco Intersight は、シスコとサードパーティの IT インフラストラクチャ向けの分析機能が組み込まれた SaaS 方式の管理プラットフォームです。Intersight Managed Mode (IMM) は、Redfish ベースの標準モデルを通じて UCS ファブリックインターコネクトシステムを管理する新しいアーキテクチャです。Intersight マネージドモードは、UCS システムの機能と Intersight のクラウドベースの柔軟性を統合し、スタンドアロンおよびファブリックインターコネクト接続システムの管理エクスペリエンスを統合します。

Cisco ベースボード管理コントローラ 2.0 REST API ガイド、リリース 2.0 デバイス コネクタが Cisco Intersight サービスへの接続を検出しない場合、次の警告を表示します。

デバイス コネクタは、Cisco Intersight に対しての接続を検出できません。設定を確認し、サーバーが Intersight インフラストラクチャ サービス ライセンスに準拠して Intersight で要求されていることを確認してください。(1/5)

次をクリックできます。[OK] をクリックします 次に移動します デバイス コネクタ 設定を構成するか、[キャンセル (Cancel)] をクリックして続行します。

警告とは別に、Cisco ベースボード管理コントローラ 2.0 REST API ガイド、リリース 2.0 画面の上部に次の静的リボンも表示します：

注：このサーバーには、Intersight インフラストラクチャ サービス ライセンス ライセンスが必要です。詳しくはこちら

詳細をクリックすると、Intersight ヘルプ センターから詳細情報を取得できます。



(注) このメッセージは、デバイス コネクタが構成されている場合は表示されません。デバイス コネクタを一度構成し、後で無効にすると、メッセージが再度表示されます。

サーバー サマリの表示

手順

ステップ 1 [Navigation] ペインから、**ダッシュボード**をクリックします。

ステップ 2 通常の システムの情報次のプロパティを表示することができます：

表 7: サーバプロパティ

名前	説明
製品名 (Product Name) field	このフィールドには、サーバの製品名が表示されます。
シリアル番号 (Serial Number) field	このフィールドには、サーバに割り当てられた一意のシリアル番号が含まれます。
UUID field	このフィールドには、サーバの UUID が含まれています。
BIOS Version field	このフィールドには、実行中の BIOS バージョンが表示されます。
説明 フィールド	このフィールドには、システムの説明が表示されます。
Asset Tag field	このフィールドには、サーバのアセットタグが含まれています。

表 8: Cisco BMC 情報

名前	説明
ホストネーム (Hostname) field	このフィールドには、サーバのホスト名が表示されます。
IPアドレス (IP Address) field	このフィールドには、サーバのIPアドレスが表示されます。

名前	説明
MAC アドレス field	このフィールドは、サーバの MAC アドレスを示します。
ファームウェアバージョン (Firmware Version) field	このフィールドは、サーバのファームウェアバージョンを示します。
[現在の時刻 (ユニバーサル) (Current Time (Universal))] field	このフィールドには、現在の万国標準時が表示されます。
Timezone field	このフィールドは、サーバのタイムゾーン設定を示します。
タイムゾーンを選択 リンク	タイムゾーンを変更できます。詳細は、 タイムゾーンの構成 (25 ページ) 。

ステップ 3 [アラート条件 (Alert Conditions)] ステータス情報次のプロパティを表示することができます :

表 9: シャーシステータス

オプション	説明
Power Status	シャーシの電源ステータスを示します。
完了後のステータス	シャーシの完了後のステータスを示します。
サーバ全体のステータス	全体のサーバのステータスを表示します。
温度	温度ステータスを示します。
DIMM全体のステータス	DIMM ステータスを表示します。
電源モジュール	電源装置のステータスを表示します。
ファン	ファン ステータスを示します。
ロケータ LED	ロケータ LED のステータスを表示します。
ストレージ全体のステータス	ストレージステータスが表示されます。

表 10: インベントリと LED

名前	説明
システム識別LED field	このフィールドには、システム識別LEDのステータスが表示されます。このLEDは、システムを物理的に識別するためにオンまたはオフに切り替えることができます。

インベントリの表示

手順

ステップ 1 [Navigation] ペインから、[システム] > [インベントリ] をクリックします。

ステップ 2 [システム (System)] タブで、次のプロパティを表示できます。

表 11: システム

名前	説明
[名前 (Name)] 列	サーバのモデル名。
説明 列	サーバモデルの簡単な説明。
[インジケータ LED (Indicator LED)] 列	各システムの識別LEDがオンかオフかを示します。
[製造業者 (Manufacturer)] 列	システムの製造業者を表示します。
[電源状態 (Power State)] 列	当該システムの現在の電力ステータスを表示します。
[シリアル番号 (Serial Number)] 列	サーバのシリアル番号。
[製品番号 (Part Number)] 列	サーバの部品番号。
[システム タイプ (System type)] 列	システムのタイプを示します。
[アセット タグ (Asset tag)] 列	システムのアセット タグを表示します。
[BIOS バージョン (BIOS Version)] 列	サーバで実行されている BIOS のバージョン。
[状態 (State)] 列	システムの現在の状態を示します。

ステップ 3 [プロセッサ (Processor)] タブで、次のプロパティを表示できます。

表 12: プロセッサ

名前	説明
[ID] コラム	各プロセッサ エントリの一意の識別子を表示します。
[製造業者 (Manufacturer)] 列	プロセッサの製造元が表示されます。
[モデル (Model)] 列	プロセッサのモデルを表示します。
[プロセッサ アーキテクチャ (Processor architecture)] 列	プロセッサのアーキテクチャを表示します。
[プロセッサ タイプ (Processor type)] 列	プロセッサのタイプを示します。
[製品番号 (Part number)] 列	プロセッサの部品番号を表示します。
[ヘルス (Health)] 列	プロセッサの現在の正常性ステータスを示します。

ステップ 4 [メモリ コントローラ (Memory Controller)] タブで、次のプロパティを表示できます。

表 13: メモリコントローラ

名前	説明
[ID] 列	メモリ コントローラの固有識別子。
[名前 (Name)] 列	メモリ コントローラの名前。
[容量 (MiB) (Capacity MiB)] 列	メモリの合計容量 (MiB 単位) 。
[製造業者 (Manufacturer)] 列	メモリ モジュールの製造元。
[SerialNumber] 列	メモリ モジュールのシリアル番号。
[製品番号 (Part number)] 列	メモリ モジュールの部品番号。
[スペア部品番号 (Spare Part Number)] 列	メモリ モジュールのスペア部品番号。
[ベース モジュール タイプ (Base module type)] 列	基本メモリ モジュールのタイプ。
[バス幅 (ビット)] 列	メモリのバス幅 (ビット単位) 。
[データ幅 (ビット)] 列	メモリのデータ幅 (ビット単位) 。
[ヘルス (Health)] 列	メモリ モジュールのヘルス ステータス。
[状態 (State)] 列	IO モジュールの動作状態
[動作速度 (MHz) (OperatingSpeed Mhz)] 列	メモリの動作速度 (MHz) 。

名前	説明
[メモリタイプ (Memory Type)]列	メモリ モジュールのタイプ。
[許可される速度 (MHz) (AllowedSpeeds MHz)]列	サポートされる速度範囲 (MHz) 。
[サービス ラベル (Service Label)]列	ID のサービス ラベル

ステップ 5 [BaseBoard] タブで、次のプロパティを表示できます。

表 14: ベース ボード : *BaseBoard* 情報

名前	説明
[名前 (Name)]列	ベース ボードの名前。
[モデル (Model)]列	ベース ボードのモデル番号。
[状態 (State)]列	ベース ボードの動作状態。
[電源状態 (Power State)]列	ベース ボードの現在の電源状態。
[アセット タグ (Asset Tag)]列	ベース ボードの識別に使用されるアセット タグ。
[製造業者 (Manufacturer)]列	ベース ボードの製造業者。
[製品番号 (Part Number)]列	ベース ボードの部品番号。
[シリアル番号 (Serial Number)]列	ベース ボードのシリアル番号。

表 15: ベース ボード : ネットワーク インターフェイス情報

名前	説明
Id 列	ネットワーク インターフェイスの一意的識別子。
[MAC アドレス (MAC Address)]列	ネットワーク インターフェイスに割り当てられた一意の Media Access Control (MAC) アドレス。
[インターフェイスが有効 (Interface Enabled)]列	ネットワーク インターフェイスが有効になっているかどうかを示します。
[HostName] 列	ネットワーク インターフェイスに関連付けられているホスト名。
[状態 (State)]列	ネットワーク インターフェイスの現在の動作状態。

表 16: ベース ボード : IPv6 アドレス情報

名前	説明
[Id] 列	IPv6 アドレスエントリの一意の識別子。
[アドレス (Address)] 列	ネットワーク インターフェイスに割り当てられている IPv6 アドレス。
[PrefixLength] 列	IPv6 アドレスのサブネットプレフィクス長。
[AddressOrigin] 列	スタティックやダイナミック割り当てなど、IPv6 アドレスの送信元。

ステップ 6 [電力 (Power)] タブで、次のプロパティを表示できます。

表 17: 電力

名前	説明
[名前 (Name)] 列	サーバ電源コンポーネントの名前。
[製造業者 (Manufacturer)] 列	電源コンポーネントの製造元。
[モデル (Model)] 列	電源コンポーネントのモデル番号
シリアル番号 列	電源コンポーネントのシリアル番号。
[製品番号 (Part Number)] 列	電源コンポーネントの部品番号。
[ヘルス (Health)] column	電源コンポーネントのヘルス ステータス。
[状態 (State)] 列	電源コンポーネントの動作状態。

ステップ 7 [温度 (Thermal)] タブで、次のプロパティを表示できます。

表 18: 温度 - ファン情報

名前	説明
[名前 (Name)] 列	コンポーネントの名前。
ヘルス (Health) 列	ファンの正常性ステータス。
[状態 (State)] 列	ファンの動作状態を確認します。
[ReadingRPM] 列	ファンの現在の速度 (RPM) 。
[下限警告 (Lower warning)] 列	ファンの速度がこの値を下回った場合に警告をトリガする下限しきい値。

名前	説明
[下限境界 (Lower critical)] 列	ファン速度がこの値を下回った場合にクリティカルアラートをトリガする下限しきい値。

表 19: 温度 : 温度情報

名前	説明
[名前 (Name)] column	温度センサーまたはモニター対象コンポーネントの名前。
[ヘルス (Health)] 列	温度センサーの正常性ステータス。
[状態 (State)] 列	温度センサーの動作状態。
[測定中 (Reading)] 列	現在の温度 (摂氏) 。
[上限警告 (Upper warning)] 列	温度がこの値を超えたときに警告をトリガする上限しきい値。
[上限境界 (Upper critical)] 列	温度がこの値を超えたときに、クリティカルアラートをトリガする上限しきい値。
[下限境界 (Lower critical)] 列	温度がこの値を下回った場合にクリティカルアラートをトリガする下限しきい値。
[下限警告 (Lower warning)] 列	温度がこの値を下回った場合に警告をトリガする下限しきい値。

ステップ 8 [PCIe デバイス (PCIe Devices)] タブで、次のプロパティを表示できます。

表 20: PCIe デバイス情報

名前	説明
[Id] 列	PCIe デバイスの固有識別子。
[DeviceClass] 列	PCIe デバイスのクラス。
[FirmwareVersion] column	PCIe デバイスにインストールされたファームウェアイメージのバージョン。
[DeviceId] column	PCIe デバイスの識別子。
[SubDeviceId] 列	PCIe デバイスのサブデバイスの識別子。
[VendorId] 列	PCIe デバイスのベンダー。
[SubVendorId] 列	PCIe デバイスのサブベンダーの識別子。

名前	説明
[状態 (State)] 列	PCIe デバイスの動作状態。

ステップ 9 [ストレージ (Storage)] タブで、次のプロパティを表示できます。

表 21: ストレージコントローラ情報

名前	説明
[MemberId] column	ストレージ FlexUtil コントローラの識別子。
[名前 (Name)] 列	ストレージ コントローラの名前。
[シリアル番号 (Serial Number)] 列	ストレージ コントローラのシリアル番号。
[モデル (Model)] 列	ストレージ コントローラのモデル
[FirmwareVersion] 列	ストレージコントローラのファームウェアバージョン
速度 (Gbs) 列	ストレージ コントローラの動作速度 (Gbps) 。
[状態 (State)] 列	ストレージ コントローラの動作可能性状態。

ステップ 10 [ネットワーク アダプタ (Network adapters)] タブで、次のプロパティを表示できます。

表 22: ネットワーク アダプタ

列	説明
[Id] 列	ネットワーク アダプタの一意的識別子。
[ヘルス (Health)] 列	ネットワーク アダプタの正常性ステータス。
アダプタ情報	
[名前 (Name)] フィールド	ネットワーク アダプタの名前。
[ベンダー (Vendor)] フィールド	ネットワーク アダプタのベンダー。
[シリアル番号 (Serial number)] field	ネットワーク アダプタのシリアル番号。
[製品番号 (Part number)] フィールド	ネットワーク アダプタの部品番号。
[製造業者 (Manufacturer)] フィールド	ネットワーク アダプタの製造元。
[モデル (Model)] フィールド	ネットワーク アダプタのモデル。
[ファームウェアのバージョン (Firmware version)] フィールド	アダプタのファームウェアバージョン

列	説明
[ステータス (状態)] フィールド	ネットワーク アダプタの動作状態。
ポート情報	
[ポート (Port)] フィールド	ネットワーク ポートの識別子。
[ポート プロトコル (Port protocol)] フィールド	ネットワーク ポートでサポートされているプロトコル。
[リンク ステータス (Link status)] フィールド	ポートの現在のリンク ステータス。
[リンク速度 (Gbps) (Link speed Gbps)] フィールド	ネットワーク リンクの速度 (Gbps 単位で測定) 。
[MAC アドレス (MAC address)] フィールド	ポートのメディアアクセスコントロール (MAC) アドレス。

ステップ 11 [GPU] タブで、次のプロパティを表示できます。

表 23: GPU 情報

名前	説明
[Id] 列	GPU の固有識別子
[製造業者 (Manufacturer)] column	GPU の製造元の名前。
ProcessorType 列	GPU で使用されるプロセッサのタイプ。
[シリアル番号 (Serial Number)] 列	GPU の固有のシリアル番号。
[製品番号 (Part Number)] 列	製造業者によって GPU に割り当てられた部品番号。
[モデル (Model)] 列	GPU のモデル名または番号。
[UUID] 列	GPU の汎用一意識別子 (UUID) 。
[バージョン (Version)] 列	GPU ハードウェアまたはファームウェアのバージョン。
[ヘルス (Health)] 列	GPU の正常性ステータス。
[状態 (State)] 列	GPU の動作状態。

ステップ 12

センサー ステータスの表示

手順

ステップ 1 [Navigation] ペインから、[システム]>[センサー]をクリックします。

ステップ 2 次のプロパティを表示することができます：

表 24: センサー

名前	説明
[名前 (Name)] column	センサーによってモニタされているコンポーネントの名前。
状態 column	モニタされているコンポーネントの動作状態。
ステータス column	モニタされているコンポーネントの全体的な正常性。
下限境界 column	クリティカルアラートをトリガするコンポーネントの下限しきい値。
下限警告 column	警告をトリガするコンポーネントの下限しきい値。
現在の値 column	コンポーネントの現在の測定値。
上限警告 column	警告をトリガするコンポーネントの上限しきい値。
上限境界 column	クリティカルアラートをトリガするコンポーネントの上限しきい値。

タイム ゾーンの構成

手順

ステップ 1 [Navigation] ペインから、ダッシュボードをクリックします。

ステップ 2 通常の Cisco BMC 情報の場合、タイムゾーンを選択。

タイムゾーンを選択 ダイアログボックスが表示されます。

ステップ3 次に **タイムゾーンを選択** ダイアログボックスで、目的のタイムゾーンを **Timezone** ドロップダウンリスト。

ステップ4 クリックして **問い合わせ**。

サーバーのブート

オプション2は、Cisco BMC 2.0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。レガシーのブート順の構成では、Cisco BMC 2.0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び替えはできません。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。

ブート順の構成を変更すると、Cisco BMC 2.0 そのサーバが次に再起動されるときに、構成されているブート順を 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。構成されたブート順は、設定が以下または BIOS 設定で再度変更されるまで Cisco BMC 2.0 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。

[現在のブート順序 (Current Boot Order)]には、サーバ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序が表示されます。

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。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 ブートを有効にすると、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、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、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。

表 25: サポートされる OS

OS	バージョン
Ubuntu サーバー	22.04
Ubuntu コア	24.04
RedHat 企業 Linux	9.4
RedHat 企業 Linux CoreOS	4.16
Rocky Linux	9.5

ブート順の構成

手順

- ステップ 1** [Navigation] ペインから、[コンピューティング] > [BIOS] をクリックします。
- ステップ 2** [All Blocks] ドロップダウンメニューを選択してレポートを選択し、結果の生成と表示を行います。ブート順序の設定 (Configure Boot Order) タブに表示されるフィールドとアイコンについて説明します。
- ステップ 3** 次の情報を確認できます。

名前	説明
UEFI セキュア ブート ドロップダウンリスト	[UEFI セキュア ブート (UEFI Secure Boot)] を無効にできます。
Boot Mode	現在のブートモードを表示します。
ワンタイムブートデバイスの設定 ドロップダウンリスト	必要なブートソースを選択できます。
ホストを即座にリブート チェックボックス	[ホストを即座にリブート (Reboot Host Immediately)] チェックボックスがオフの場合、サーバーはすぐに関機され、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。

名前	説明
現在のブート順 エリア リスト	現在のブート順序を表示します。
予測されるブート順 リスト	このリスト内の項目をドラッグすることで、コンポーネントのブート順序を並べ替えることができます。

ステップ4 登録手続きを開始するには、**変更の保存**。

サーバーの実際のブート順の表示

手順

- ステップ1 [Navigation] ペインから、[コンピューティング]>[BIOS]をクリックします。
- ステップ2 [All Blocks] ドロップダウンメニューを選択してレポートを選択し、結果の生成と表示を行います。ブート順序の設定 (Configure Boot Order) タブに表示されるフィールドとアイコンについて説明します。
- ステップ3 通常の [現在のブート順 エリア (Current Boot Order Area)] リストの下で、現在の実際のブート順序を確認できます。

UEFI セキュア ブートの有効化または無効化

手順

- ステップ1 [Navigation] ペインから、[コンピューティング]>[BIOS]をクリックします。
- ステップ2 [All Blocks] ドロップダウンメニューを選択してレポートを選択し、結果の生成と表示を行います。ブート順序の設定 (Configure Boot Order) タブに表示されるフィールドとアイコンについて説明します。
- ステップ3 [バーチャルアカウント (Virtual Account)] ドロップダウン リストから、**UEFI セキュア ブート** ドロップダウンリストから、**有効** または **ディセーブル**。
- ステップ4 登録手続きを開始するには、**変更の保存**。

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。

手順

- ステップ1 [Navigation] ペインから、[コンピューティング]>[BIOS]をクリックします。
- ステップ2 [All Blocks] ドロップダウンメニューを選択してレポートを選択し、結果の生成と表示を行います。ブート順序の設定（Configure Boot Order）タブに表示されるフィールドとアイコンについて説明します。
- ステップ3 [バーチャルアカウント（Virtual Account）] ドロップダウンリストから、[構成済みのワンタイム ブート デバイス（Configured one time boot device）] ドロップダウンで、オプションを選択します。
- ステップ4 （任意）※ ホストを即座にリブート チェックボックスをオンにします。
- ステップ5 登録手続きを開始するには、変更の保存。

BIOS トークン

I/O BIOS パラメータの構成



(注) 記載されている BIOS のパラメータは、サーバーによって異なります。

手順

- ステップ1 [Navigation] ペインから、[コンピューティング]>[BIOS]をクリックします。
- ステップ2 [All Blocks] ドロップダウンメニューを選択してレポートを選択し、結果の生成と表示を行います。[BIOS の設定（Configure BIOS）] タブに表示されるフィールドとアイコンについて説明します。
- ステップ3 [All Blocks] ドロップダウンメニューを選択してレポートを選択し、結果の生成と表示を行います。I/O タブに表示されるフィールドとアイコンについて説明します。

次のトークンを表示または、アップデートすることができます：

BIOS トークン	説明
ホストを即座にリブート チェックボックス	[ホストを即座にリブート（Reboot Host Immediately）] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しいBIOS設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。

BIOS トークン	説明
IPv4 PXEサポート ドロップダウンリスト	<p>PXE の IPv4 サポートを有効または無効にします。次のいずれかになります</p> <ul style="list-style-type: none"> • ディセーブル : IPv4 PXE のサポートは利用できません。 • 有効 : IPv4 PXE のサポートを常に利用できます。
IPv4 HTTPサポート ドロップダウンリスト	<p>HTTP の IPv4 サポートを有効または無効にします。次のいずれかになります。</p> <ul style="list-style-type: none"> • ディセーブル : IPv4 HTTP サポートは使用できません。 • 有効 : IPv4 HTTP サポートを常に使用できます。
IPv6 PXE サポート ドロップダウンリスト	<p>PXE の IPv6 サポートを有効または無効にします。次のいずれかになります。</p> <ul style="list-style-type: none"> • ディセーブル : IPv6 PXE のサポートは利用できません。 • 有効 : IPv6 PXE のサポートを常に利用できます。
IPv6 HTTP サポート ドロップダウンリスト	<p>HTTP の IPv6 サポートを有効または無効にします。次のいずれかになります。</p> <ul style="list-style-type: none"> • ディセーブル : IPv6 HTTP サポートは使用できません。 • 有効 : IPv6 HTTP サポートを常に使用できます。

BIOS トークン	説明
PCIE リンク スピード機能 ドロップダウンリスト	PCIExpress インターフェイスが動作できる最大速度を決定します。 <ul style="list-style-type: none"> • Auto : 接続されたデバイスの機能とシステム要件に基づいて、最適な PCI Express リンク速度を自動的に選択します。 • GEN1 : PCI Express リンクを第 1 世代の速度である 2.5 GT/s (1 秒あたりのギガの転送数) で動作するように設定します。 • GEN2 : PCI Express リンクを 5.0 GT/s の第 2 世代の速度で実行するように設定します。 • GEN3 : 第 3 世代 (8.0 GT/s) で PCI Express リンク速度を確立します。 • GEN4 : 16.0 GT/s の第 4 世代の速度で PCI Express リンクを動作します。 • GEN5 : PCI Express リンクを第 5 世代の速度 (32.0 GT/s) に設定し、リストされているオプションの中で最大の帯域幅を提供します。
[SR-IOV のサポート (SR-IOV Support)] ドロップダウンリスト	SR-IOV 機能により、PCIe デバイスは複数の個別の物理 PCIe デバイスのように見えます。次のいずれかになります。 <ul style="list-style-type: none"> • ディセーブル : SR-IOV 機能は無効です。 • 有効 : SR-IOV 機能は有効です。

ステップ 4 [Save]をクリックします。

サーバ管理 BIOS パラメータの構成



(注) 記載されている BIOS のパラメータは、サーバーによって異なります。

手順

ステップ 1 [Navigation] ペインから、[コンピューティング]>[BIOS]をクリックします。

ステップ 2 [All Blocks] ドロップダウンメニューを選択してレポートを選択し、結果の生成と表示を行います。[BIOS の設定 (Configure BIOS)] タブに表示されるフィールドとアイコンについて説明します。

ステップ 3 [All Blocks] ドロップダウンメニューを選択してレポートを選択し、結果の生成と表示を行います。サーバ管理 タブに表示されるフィールドとアイコンについて説明します。

次のトークンを表示または、アップデートすることができます：

BIOS トークン	説明
ホストを即座にリブート チェックボックス	[ホストを即座にリブート (Reboot Host Immediately)] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
コンソールリダイレクション (Console Redirection) ドロップダウンリスト	POST および BIOS のブート中に、シリアルポートをコンソールリダイレクションで使用できるようにします。OS 起動後は、コンソールのリダイレクトが関係なくなります。次のいずれかになります。 <ul style="list-style-type: none"> • 有効：POST 中にコンソールリダイレクションをイネーブルにします。 • ディセーブル：POST 中にコンソールリダイレクションは発生しません。
[ターミナルタイプ (Terminal Type)] ドロップダウンリスト	コンソールリダイレクションに使用される文字フォーマットのタイプ。次のいずれかになります。 <ul style="list-style-type: none"> • PC-ANSI：PC-ANSI 端末フォントが使用されます。 • VT100：サポートされている VT100 ビデオ端末とその文字セットが使用されます。 • VT100-PLUS：サポートされている VT100-plus ビデオ端末とその文字セットが使用されます。 • VT-UTF8：UTF-8 文字セットのビデオ端末が使用されます。

BIOS トークン	説明
1秒あたりのビット数 ドロップダウンリスト	<p>この設定は、シリアル通信のデータ伝送速度（ビット/秒 (bps)）を決定します。これは、通信チャンネルを介してデータが送信および受信されるレートを定義します。</p> <ul style="list-style-type: none"> • 9600 • 19200 • 38400 • 57600 • 115200 • 230400 • 460800 • 921600
Flow Control ドロップダウンリスト	<p>フロー制御にハンドシェイクプロトコルを使用するかどうかを設定します。送信要求/クリア ツーセンド (RTS/CTS) を使用すると、隠れた端末の問題が原因で発生する可能性がある、フレームコリジョンを減らすことができます。次のいずれかになります。</p> <ul style="list-style-type: none"> • なし：フロー制御は使用されません。 • ハードウェア RTS/CTS：RTS/CTS がフロー制御に使用されます。
[FRB-2 タイマー (FRB-2 Timer)] ドロップダウンリスト	<p>POST 中にシステムがハングした場合に、システムを回復するために FRB2 タイマーを使用するかどうかを設定します。次のいずれかになります。</p> <ul style="list-style-type: none"> • ディセーブル：FRB2 タイマーは使用されません。 • 有効：POST 中に FRB2 タイマーが開始され、必要に応じてシステムの回復に使用されます。

BIOS トークン	説明
OS Watchdog Timer ドロップダウンリスト	<p>BIOS が指定されたタイムアウト値でウォッチドッグタイマーをプログラムするかどうか。次のいずれかになります。</p> <ul style="list-style-type: none"> • ディセーブル：サーバのブートにかかる時間をトラッキングするためにウォッチドッグタイマーは使用されません。 • 有効：サーバのブートにかかる時間をウォッチドッグタイマーでトラッキングします。サーバのブートが [OS ブートウォッチドッグタイマータイムアウト (OS Boot Watchdog Timer Timeout)] フィールドで指定された時間内に完了しない場合は、Cisco BMC によってエラーがログに記録され、[OS ブートウォッチドッグポリシー (OS Boot Watchdog Policy)] フィールドで指定されたアクションが実行されます。
[OS WTD タイマータイムアウト (OS Wtd Timer Timeout)] フィールド	<p>OS が指定された時間内にブートしない場合、OS ウォッチドッグタイマーの期限が切れ、システムはタイマーポリシーに基づいてアクションを実行します。1 ~ 30 の整数を入力します。</p>
[OS Wtd タイマーポリシー (OS Wtd Timer Policy)] ドロップダウンリスト	<p>ウォッチドッグタイマーが切れた場合にシステムで実行されるアクション。次のいずれかになります。</p> <ul style="list-style-type: none"> • Do Nothing：OS の起動中にウォッチドッグタイマーが期限切れになった場合、アクションは実行されません。これにより、システムは介入なしで現在の状態を継続できます。 • Reset：OS のブート中にウォッチドッグタイマーが切れた場合、サーバーはリセットされます。 • Power Down：OS のブート中にウォッチドッグタイマーの期限が切れた場合、サーバの電源がオフになります。 • Power Cycle：OS のブート中にウォッチドッグタイマーが切れると、サーバの電源がオフになってからオンに戻り、システムを効果的にリブートして潜在的な問題に対処します。

ステップ4 [保存 (Save)] をクリックします。

セキュリティ BIOS パラメータの構成



(注) 記載されている BIOS のパラメータは、サーバーによって異なります。

手順

ステップ1 [Navigation] ペインから、[コンピューティング]>[BIOS]をクリックします。

ステップ2 [All Blocks] ドロップダウンメニューを選択してレポートを選択し、結果の生成と表示を行います。[BIOS の設定 (Configure BIOS)] タブに表示されるフィールドとアイコンについて説明します。

ステップ3 [All Blocks] ドロップダウンメニューを選択してレポートを選択し、結果の生成と表示を行います。セキュリティ タブに表示されるフィールドとアイコンについて説明します。

次のトークンを表示または、アップデートすることができます：

BIOS トークン	説明
ホストを即座にリブート チェックボックス	[ホストを即座にリブート (Reboot Host Immediately)] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しいBIOS設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
セキュリティデバイスのサポート ドロップダウンリスト	このオプションを使用すると、システムのセキュリティ デバイス サポートを制御できます。次のいずれかになります。 <ul style="list-style-type: none"> • ディセーブル：このオプションは無効です。 • 有効HTTP サーバーは無効です。

BIOS トークン	説明
[TPM State] ドロップダウンリスト	<p>この機能は、トラステッドプラットフォームモジュール (TPM) のステータスを制御します。TPM は、暗号キー用にセキュアなストレージを提供し、プラットフォーム整合性チェックを実行することによって、システムセキュリティを強化するために使用されるハードウェアベースのセキュリティデバイスです。</p> <ul style="list-style-type: none"> • 有効 : TPM をアクティブにして、キー管理やシステム整合性の確認などのセキュリティ機能を実行できるようにします。 • ディセーブル : TPM を非アクティブ化し、セキュリティ関連のタスクを実行できないようにします。
SHA256 PCRバンク ドロップダウンリスト	<p>SHA256 PCR バンクを有効または無効にします。次のいずれかになります。</p> <ul style="list-style-type: none"> • ディセーブル : サーバーではこの機能が使用されません。 • 有効 : サーバーはこの機能を使用します。
SHA384 PCR バンク ドロップダウンリスト	<p>プラットフォーム構成レジスタ (PCR) は、TPM 内のメモリ位置です。複数の PCR をまとめて PCR バンクと呼びます。セキュアハッシュアルゴリズム 384 ビットまたは SHA-384PCR バンクでは、TPM セキュリティを有効または無効にすることができます。</p> <p>次のいずれかになります。</p> <ul style="list-style-type: none"> • ディセーブル : サーバーではこの機能が使用されません。 • 有効 : サーバーはこの機能を使用します。
保留中の操作 ドロップダウンリスト	<p>トラステッドプラットフォームモジュール (TPM) Pending Operation オプションを使用すると、保留中の操作のステータスを制御できます。次のいずれかになります。</p> <ul style="list-style-type: none"> • なしアクション はありません。 • TpmClear 保留中の操作をクリアします。

BIOS トークン	説明
[ランタイム変数のパスワード保護 (Password protection of Runtime Variables)] ドロップダウンリスト	<p>この機能では、アクセスまたは変更にパスワードを要求することで、ランタイム変数を保護します。操作中に重要な設定に対する不正な変更を防止することにより、システムセキュリティを強化します。</p> <ul style="list-style-type: none"> • 有効：ランタイム変数にアクセスして変更する場合パスワードを要求します。システム設定に対する不正な変更を防ぐためのセキュリティレイヤが追加されます。 • ディセーブル：パスワードなしでランタイム変数にアクセスして変更できます。セキュリティについての問題があまりない環境に適している場合があります。

ステップ 4 [保存 (Save)] を [Save]。

メモリ BIOS パラメータの構成



(注) 記載されている BIOS のパラメータは、サーバによって異なります。

手順

ステップ 1 [Navigation] ペインから、[コンピューティング] > [BIOS] をクリックします。

ステップ 2 次の [BIOS の構成 (Configure BIOS)] タブを選択します。

ステップ 3 次の [I/O] タブを選択します。

次のトークンを表示または、アップデートすることができます：

BIOS トークン	説明
[ホストを即座にリブート (Reboot Host Immediately)] チェックボックス	<p>がオフの場合、サーバはすぐにリブートされ、新しい BIOS 設定が有効になります。それ以外の場合は、サーバが手動でリブートされるまで変更は保存されます。</p>

BIOS トークン	説明
[SMEE] ドロップダウン リスト	<p>プロセッサで、メモリの暗号化サポートを実現する Secure Memory Encryption Enable (SMEE) 機能を使用するかどうかを指定します。次のいずれかになります。</p> <ul style="list-style-type: none"> • [自動 (Auto)] : これらのアドレスのマッピング方法を CPU で決定します。 • [無効 (Disabled)] : プロセッサで SMEE 機能を使用しません。 • [有効 (Enabled)] : プロセッサで SMEE 機能を使用します。
[SNP メモリ (RMP テーブル) カバレッジ (SNP Memory (RMP Table) Coverage)] ドロップダウン リスト ドロップダウン リスト	<p>SNP メモリ カバレッジを構成できます。次のいずれかになります。</p> <ul style="list-style-type: none"> • [自動 (Auto)] : システムがメモリ カバレッジを決定します。 • [無効 (Disabled)] : プロセッサはこの機能を使用しません。 • [有効 (Enabled)] : この機能は次を経由して有効になります。 • [カスタム (Custom)] : カスタムサイズは、カバーする SNP メモリ サイズで定義できます。
[L1 バーストプリフェッチモード (L1 Burst Prefetch Mode)] ドロップダウン リスト	<p>この設定は、レベル1 (L1) キャッシュのプリフェッチ動作を制御します。事前にデータをロードすることで処理効率を向上させることができます。</p> <ul style="list-style-type: none"> • [有効 (Enable)] : バーストプリフェッチをアクティブにします。データを L1 キャッシュにプリロードすることでパフォーマンスが向上する可能性があります。 • [無効 (Disable)] : バーストプリフェッチを非アクティブにします。これによりパフォーマンスが低下する可能性があります。電力を節約し、不要なデータ取得を減らすことができます。 • [自動 (Auto)] : システムのワークロードと条件に基づいて L1 バーストプリフェッチを自動的に管理し、パフォーマンスと効率を最適化します。

BIOS トークン	説明
<p>[ソケットごとの NUMA ノード (NUMA nodes per socket)] ドロップダウン リスト</p>	<p>ソケットごとにメモリ NUMA ドメインを構成できます。次のいずれかになります。</p> <ul style="list-style-type: none"> • [自動 (Auto)] : チャンネル数を自動的に設定します。 • [NPS0] : システムごとの NUMA ノード数を 1 にします。 • [NPS1] : ソケットごとの NUMA ノード数を 1 にします。 • [NPS2] : ソケットごとの NUMA ノード数を 2 にし、SoC の左半分と右半分に 1 つずつにします。 • [NPS4] : ソケットごとの NUMA ノード数を 4 にし、クワドラントごとに 1 つにします。
<p>[メモリ インターリーブ (Memory interleaving)] ドロップダウン リスト</p>	<p>メモリ インターリーブを無効にできます。ソケットあたりの NUMA ノードは、この設定に関係なく適用されることに注意してください。次のいずれかになります。</p> <ul style="list-style-type: none"> • [自動 (Auto)] : 機能を自動モードに設定します。 • [有効 (Enabled)] : この機能は次を経由して有効になります。 • [無効 (Disabled)] : サポートは無効になっています。
<p>[チップ選択インターリーブ (Chipselect Interleaving)] ドロップダウン リスト</p>	<p>ノード 0 に選択する DRAM チップ経由でメモリ ブロックがインターリーブされるかどうか。次のいずれかになります。</p> <ul style="list-style-type: none"> • [無効 (Disabled)] : チップの選択は、メモリ コントローラ内でインターリーブされません。 • [自動 (Auto)] : CPU でチップセレクトのインターリーブの方法を自動的に決定します。

BIOS トークン	説明
<p>[BankSwapMode] ドロップダウン リスト</p>	<p>メモリバンクのスワップを制御して、パフォーマンスを最適化したり、特定のメモリ構成を管理したりできます。メモリアクセスパターンを改善したり、ハードウェア要件に適応したりするのに役立ちます。</p> <ul style="list-style-type: none"> • [自動 (Auto)] : システム要件と機能に基づいて、最適なバンクスワップ構成が自動的に選択されます。 • [無効 (Disable)] : バンク スワッピングを防止し、メモリバンク設定を変更せずに初期設定のままにします。 • [スワップCPU (Swap CPU)] : CPUのパフォーマンスとアクセスパターンを最適化するように調整されたメモリ バンク スワップを有効にします。
<p>[DRAM リフレッシュ レート (DRAM Refresh Rate)] ドロップダウン リスト</p>	<p>この設定は、データの整合性を維持するために DRAMセルをリフレッシュする間隔を決定します。リフレッシュレートを低くするとパフォーマンスは向上しますが、消費電力が増加する可能性があります。一方、レートを高くするとデータ保持期間が長くなります。次のいずれかになります。</p> <ul style="list-style-type: none"> • 3.9 マイクロ秒 • 1.95 マイクロ秒

BIOS トークン	説明
<p>[DDR 修復 BIST (DDR Healing BIST)] ドロップダウンリスト</p>	<p>これは、DDR メモリ モジュール内のメモリ障害を特定して修復するために使用される診断ツールです。一連のセルフテストを実行することで、システムは障害のあるセルを検出して機能の復元を試みることができるため、メモリの信頼性とパフォーマンスが向上します。</p> <ul style="list-style-type: none"> • [無効 (Disabled)] : DDR 修復 BIST 機能を無効にし、メモリ診断テストが実行されないようにします。 • [PMU メモリ BIST (PMU Mem BIST)] : 障害検出のためにパフォーマンス モニタリング ユニットベースのメモリ組み込みセルフテストを有効にします。 • [自己修復メモリ BIST (Self-Healing Mem BIST)] : 自己修復機能をアクティブにして、メモリ障害を自動的に検出して修復します。 • [PMU および自己修復 Mem BIST (PMU and Self-Healing Mem BIST)] : PMU ベースのテストと自己修復テストを組み合わせ、包括的なメモリの診断と修復を行います。
<p>[DRAM ブート時間ポストパッケージ修復 (DRAM Boot Time Post Package Repair)] ドロップダウンリスト</p>	<p>このオプションを使用すると、システムはブートプロセス中に DRAM で修復を試み、検出された障害を修正できます。これにより、メモリの整合性と信頼性が確保されます。</p> <ul style="list-style-type: none"> • [有効 (Enabled)] : ブート時の修復プロセスをアクティブにして、システムが起動時にメモリの問題を特定して修正できるようにします。 • [無効 (Disabled)] : ブート時修復プロセスを無効にし、システム起動時の自動 DRAM 障害修正をスキップします。
<p>ランタイム ポスト パッケージ修復 ドロップダウンリスト</p>	<p>これは、実行時にプロセッサのパッケージを修復するシステムの機能に関連する特定の構成の設定です。</p> <ul style="list-style-type: none"> • [有効 (Enabled)] : プロセッサで機能を使用します。 • [無効 (Disabled)] : プロセッサで機能を使用しません。

BIOS トークン	説明
[DRAMスクラブ時間 (DRAM Scrub Time)] ドロップダウンリスト	<p>値を選択して、メモリ全体をスクラブする時間を示します。次のいずれかになります。</p> <ul style="list-style-type: none"> • [自動 (Auto)] : 機能を自動モードに設定します。 • [無効 (Disabled)] : サポートは無効になっています。 • 1 時間 • 4 時間 • 8 時間 • 16 時間 • 24 時間 • 48 時間
TSME ドロップダウンリスト	<p>透過的セキュアメモリ暗号化 (TSME) を有効にすることができます。次のいずれかになります。</p> <ul style="list-style-type: none"> • [自動 (Auto)] : 機能の使用は自動に設定されます。 • [無効 (Disabled)] : プロセッサで TSME 機能を使用しません。 • [有効 (Enabled)] : プロセッサで TSME 機能を使用します。
[SEV-SNP サポート (SEV-SNP Support)] ドロップダウンリスト	<p>セキュア ネスティッド ページング機能を有効にできます。次のいずれかになります。</p> <ul style="list-style-type: none"> • [無効 (Disabled)] : プロセッサで SEV-SNP 機能を使用しません。 • [有効 (Enabled)] : プロセッサで SEV-SNP 機能を使用します。 • [自動 (Auto)] : システムの機能と要件に基づいて SEV-SNP 機能を自動的に有効にし、手動で構成することなく仮想マシンのセキュリティを最適化します。

BIOS トークン	説明
<p>[IOMMU] ドロップダウンリスト</p>	<p>出入力メモリ管理ユニット (IOMMU) により、AMD プロセッサが物理アドレスへ仮想アドレスをマッピングすることが可能です。次のいずれかになります。</p> <ul style="list-style-type: none"> • [自動 (Auto)] : これらのアドレスのマッピング方法を CPU で決定します。 • [無効 (Disabled)] : IOMMU は使用されません。 • [有効 (Enabled)] : IOMMU によりアドレスマッピングを行います。
<p>[4G 以上の復号 (Above 4G Decoding)] ドロップダウンリスト</p>	<p>4GB を超える MMIO を有効もしくは無効にします。次のいずれかになります。</p> <ul style="list-style-type: none"> • [無効 (Disabled)] : サーバでは 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングしません。 • [有効 (Enabled)] : サーバで 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングします。PCI デバイスが 64 ビット対応でも、レガシーなオプション ROM を使用する場合は、この設定を有効にしても正しく機能しない場合があることに注意してください。
<p>[BME DMA 緩和 (BME DMA Mitigation)] ドロップダウンリスト</p>	<p>不正な外部 DMA からの脅威を緩和する PCI BME ビットを無効にできます。次のいずれかになります。</p> <ul style="list-style-type: none"> • [無効 (Disabled)] : PCI BME ビットは BIOS で無効になっています。 • [有効 (Enabled)] : PCI BME ビットは BIOS で有効になっています。

ステップ 4 [保存 (Save)] をクリックします。

プロセッサの BIOS パラメータの構成



(注) 記載されている BIOS のパラメータは、サーバーによって異なります。

手順

ステップ 1 [Navigation] ペインから、[コンピューティング]>[BIOS]をクリックします。

ステップ 2 以下の [BIOS の構成 (Configure BIOS)] タブを選択します。

ステップ 3 以下の [電源/パフォーマンス (Power/Performance)] タブを選択します。

次のトークンを表示またはアップデートすることができます：

BIOS トークン	説明
ホストを即座にリブート チェックボックス	[ホストを即座にリブート (Reboot Host Immediately)] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
[SVM モード (SMT Mode)] ドロップダウン リスト	プロセッサが AMD セキュア仮想マシンテクノロジーを使用するかどうか。次のいずれかを選択できます。 <ul style="list-style-type: none"> • [ディセーブル (Disabled)] : プロセッサで SVM テクノロジーを使用しません。 • [有効 (Enabled)] : プロセッサで SVM テクノロジーを使用します。
ストリーミングストア制御 ドロップダウン リスト	ストリーミングストア機能を有効にします。次のいずれかになります。 <ul style="list-style-type: none"> • [自動 (Auto)] : 自動モードに設定します。 • [ディセーブル (Disabled)] 機能が無効になっています。 • [有効 (Enabled)] : 機能が有効になっています。

BIOS トークン	説明
ローカルAPICモード ドロップダウン リスト	<p>この機能は、CPU内の割り込みのシグナリングと優先順位付けを管理するローカルの高度なプログラマブル割り込みコントローラ (APIC) のモードを構成します。次のいずれかになります。</p> <ul style="list-style-type: none"> • [自動 (Auto)] : 自動モードに設定します。 • [XAPIC] : XAPIC モードに設定します。 • [X2APIC] : X2APIC モードに設定します。
[AVX512] ドロップダウン リスト	<p>AVX512 BIOS 設定は、AVX512 命令セット拡張の使用を有効または無効にします。これは、特定の Intel® プロセッサで使用される高度なベクトル拡張であり、重い計算タスクのパフォーマンスを向上させます。</p> <p>この設定を調整すると、一部のソフトウェアとの互換性と安定性に影響を与え、CPUの電力消費と発熱量に影響を与える可能性があります。</p> <p>AVX512 を有効または無効化にします。次のいずれかになります。</p> <ul style="list-style-type: none"> • [自動 (Auto)] : 自動モードに設定します。 • [ディセーブル (Disabled)] 機能が無効になっています。 • [有効 (Enabled)] : 機能が有効になっています。
[DownCore] ドロップダウン リスト	<p>アクティブなプロセッサコアの数を設定して、ワークロードの要件に従ってパフォーマンスと電力消費を最適化します。</p> <ul style="list-style-type: none"> • [有効化オプション (Enablement Option)] : アクティブコアの事前定義された構成から選択でき、特定のパフォーマンスまたは電力の目標に合わせてコアの使用を最適化するプロセスを簡素化します。 • [ビットマップ (Bitmap)] : ビットマップを介してアクティブコアのカスタム選択を可能にし、カスタマイズされたパフォーマンスチューニングのためにコアを有効または無効にする正確な制御を提供します。

BIOS トークン	説明
[SMT 制御 (SMT Control)] ドロップダウンリスト	<p>プロセッサで AMD Simultaneous MultiThreading テクノロジーを使用するかどうかを指定します。このテクノロジーでは、マルチスレッドソフトウェアアプリケーションのスレッドを各プロセッサ内で並列に実行できます。次のいずれかになります。</p> <ul style="list-style-type: none"> • [自動 (Auto)] : プロセッサは、マルチスレッドの並列実行を許可します。 • [ディセーブル (Disabled)] : プロセッサで SMT モードを使用しません。 • [有効 (Enabled)] : プロセッサで SMT モードを使用します。
[CCD 制御 (CCD Control)] ドロップダウンリスト	<p>システムで有効にしたい CCD の数を指定できます。次のいずれかになります。</p> <ul style="list-style-type: none"> • [自動 (Auto)] : プロセッサによって提供される最大数の CCD が有効になります。 • 2 CCD • 3 CCD • 4 CCD • 6 CCD
NUMA ドメインとしての ACPI SRAT L3 キャッシュ ドロップダウンリスト	<p>各 CCX がそのオン ドメインにあると宣言されている物理ドメインの上に仮想ドメインのレイヤーを作成します。次のいずれかになります。</p> <ul style="list-style-type: none"> • [自動 (Auto)] : 自動モードに設定します。 • [ディセーブル (Disabled)] : ドメイン構成に NPS 設定を使用します。 • [有効 (Enabled)] : 各 CCX を独自のドメインにあると宣言します。

BIOS トークン	説明
[3リンク xGMI 最大速度 (3-link xGMI max speed)] ドロップダウン リスト	このオプションは、18 Gbps XGMI リンク速度を有効にします。次のいずれかになります。 <ul style="list-style-type: none"> • [自動 (Auto)] : 自動モードに設定します。 • 20 Gbps : 20Gbps に設定します。 • 25 Gbps : 25Gbps に設定します。 • 32 Gbps : 32Gbps に設定します。
[パワー ダウンの有効化 (Power Down Enable)] ドロップダウン リスト	この設定は、システムがアイドル状態のとき、または使用率が低いときにメモリ (RAM) を低電力状態にするかどうかを制御します。通常、この設定を有効にすると、RAM の電力消費が少なくなり、エネルギーが節約され、発熱量が減少する可能性があります。無効にすると、RAM の電力が完全に維持され、ウェイクアップ時間が短縮される可能性があります。電力消費は高くなります。次のいずれかになります。 <ul style="list-style-type: none"> • [自動 (Auto)] : 自動モードに設定します。 • [ディセーブル (Disabled)] 機能が無効になっています。 • [有効 (Enabled)] : 機能が有効になっています。
[APBDIS] ドロップダウン リスト	SMU の APB 無効化の値を選択できます。次のいずれかになります。 <ul style="list-style-type: none"> • 0 : SMU への ApbDis をクリアします • 1 : SMU への ApbDis を設定します。 • [自動 (Auto)] : CPU が値を判断します。

ステップ 4 [保存 (Save)] をクリックします。

電源とパフォーマンスの BIOS パラメータの構成



(注) 記載されている BIOS のパラメータは、サーバーによって異なります。

手順

- ステップ 1 [Navigation] ペインから、[コンピューティング]>[BIOS]をクリックします。
- ステップ 2 [All Blocks] ドロップダウンメニューを選択してレポートを選択し、結果の生成と表示を行います。[BIOS の設定 (Configure BIOS)] タブに表示されるフィールドとアイコンについて説明します。
- ステップ 3 [All Blocks] ドロップダウンメニューを選択してレポートを選択し、結果の生成と表示を行います。電源/パフォーマンス タブに表示されるフィールドとアイコンについて説明します。

次のトークンを表示または、アップデートすることができます：

BIOS トークン	説明
[ホストを即座にリブート] チェックボックス	[ホストを即座にリブート (Reboot Host Immediately)] チェックボックスがオフの場合、サーバーはすぐにリブートされ、新しい BIOS 設定が有効になります。そうでない場合、変更内容はサーバーが手動でリブートされるまで保存されます。
[コア パフォーマンス ブースト (Core Performance Boost)] ドロップダウンリスト	AMD プロセッサがアイドル状態 (ほとんど使用されていない状態) のときにコアの周波数を上げるかどうかを指定します。次のいずれかになります。 <ul style="list-style-type: none"> • [自動 (Auto)] : パフォーマンスをブーストする方法を CPU で自動的に決定します。 • [ディセーブル (Disabled)] : CPU により自動的にブーストパフォーマンスが決定されます。
[グローバル C-State 制御 (Global C-state Control)] ドロップダウンリスト	AMD プロセッサが IO ベースの C ステートおよび DFC ステートを制御するかどうかに関係なく、これは次のうちいずれかになります。 <ul style="list-style-type: none"> • [自動 (Auto)] : CPU で IO ベースの C ステートの生成方法を自動的に決定します。 • [ディセーブル (Disabled)] : グローバル C ステートの制御が無効になります。 • [イネーブル (Enabled)] : グローバル C ステートの制御が有効になります。

BIOS トークン	説明
<p>[L1 Stream HW Prefetcher] ドロップダウンリスト</p>	<p>プロセッサで、AMD ハードウェア プリフェッチャが必要に応じてデータおよび命令ストリームをメモリから取得し、L1 キャッシュに入れることを許可するかどうか。次のいずれかになります。</p> <ul style="list-style-type: none"> • [自動 (Auto)] : CPU は、I/O デバイスからプロセッサ キャッシュにデータを配置する方法を決定します。 • [ディセーブル (Disabled)] : ハードウェア プリフェッチャは使用しません。 • [イネーブル (Enabled)] : プロセッサで、キャッシュの問題が検出されたときにプリフェッチャを使用します。
<p>[L2 Stream HW Prefetcher] ドロップダウンリスト</p>	<p>プロセッサで、AMD ハードウェア プリフェッチャが必要に応じてメモリからデータおよび命令ストリームを取得し、L2 キャッシュに入れることを許可するかどうかを指定します。次のいずれかになります。</p> <ul style="list-style-type: none"> • [自動 (Auto)] : CPU は、I/O デバイスからプロセッサ キャッシュにデータを配置する方法を決定します。 • [ディセーブル (Disabled)] : ハードウェア プリフェッチャは使用しません。 • [イネーブル (Enabled)] : プロセッサで、キャッシュの問題が検出されたときにプリフェッチャを使用します。
<p>決定論の有効化 ドロップダウンリスト</p>	<p>この機能により、システムはリソース割り当てとパフォーマンス特性を管理して、選択したモードに基づいて一貫した結果を達成できます。</p> <ul style="list-style-type: none"> • [電力 (Power)] : 予測可能なパフォーマンスレベルを維持しながら、電力効率を優先するようにシステムを最適化します。 • [パフォーマンス (Performance)] : パフォーマンスの一貫性を最大化するようにシステムを設定します。ただし、消費電力は高くなりますが、

ステップ4 [保存 (Save)]をクリックします。

電力ポリシーの設定

電力制限

電力制限によって、サーバー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。



(注) 電力制限は CPU にのみ適用されます。メモリやストレージなどの他のサーバコンポーネントは、パワー キャッピングの範囲に含まれません。

CPU 電力制限の有効化

手順

ステップ1 [Navigation] ペインから、システム > 電源管理をクリックします。

ステップ2 通常の 電力制限値(単位: ワット)で、必要な電力制限値をワット単位で入力します。

値が最小キャップ制限と最大キャップ制限の間にあることを確認します。

ステップ3 [保存 (Save)]を [Save] クリックして電源制限設定を適用します。

CPU 電力構成の表示

手順

ステップ1 [Navigation] ペインから、システム > 電源管理をクリックします。

ステップ2 次のプロパティを表示することができます：

名前	説明
[名前 (Name)] column	コンポーネントまたはデバイスを識別します。
消費電力 column	現在の電力の使用状況を表示します。
電力制限 column	コンポーネントに設定されている最大電力制限を示します。
下限 column	最小許容電力制限を表示します。
上限 column	最大許容電力制限を表示します。

電力復元ポリシーの構成

手順

ステップ 1 [Navigation] ペインから、[コンピューティング]>[電力復元ポリシー]をクリックします。

ステップ 2 リスト **電源復旧ポリシー** エリアをクリックして適切な値を選択します。

- **常時稼働**：電源喪失前の状態に関係なく、電源が投入されるたびにシステムの電源が自動的にオンになります。このオプションを使用すると、電力が供給可能になるとすぐにサーバが動作を再開します。
- **常にオフ**：以前の状態に関係なく、電源が入っている場合、システムの電源はオフのままです。このオプションでは、電源喪失後にシステムの電源をオンにするために手動による介入が必要です。
- **最終の状態**：電源を入れると、システムは以前の電源状態を復元します。電源を失う前にシステムの電源がオンになっていた場合は、電源をオンにします。電源がオフになっている場合は、電源がオフのままになります。

ステップ 3 登録手続きを開始するには、**設定の保存**。



第 4 章

ユーザー アカウントの管理

- ユーザ管理 (53 ページ)
- LDAP 設定 (59 ページ)
- ユーザ セッション (62 ページ)

ユーザ管理

ユーザーの追加

手順

ステップ 1 [Navigation] ペインから、[管理] > [ユーザー管理] をクリックします。

ステップ 2 ユーザー管理 タブを選択します。

ステップ 3 登録手続きを開始するには、ユーザーの追加。

ユーザーの追加 ウィンドウが表示されます。

ステップ 4 次にユーザーの追加 ウィンドウで次のプロパティを更新します。

名前	説明
アカウントステータス オプション ボタンを選択します	<p>[All Blocks] ドロップダウン メニューを選択してレポートを選択し、結果の生成と表示を行います。有効 [有効 (Enabled)] ラジオ ボタンを選択し、アカウントを即時にアクティブ化します。</p> <p>[All Blocks] ドロップダウン メニューを選択してレポートを選択し、結果の生成と表示を行います。ディセーブル [無効化 (Disabled)] ラジオ ボタンを選択し、アクティベーション無しでアカウントを作成します。</p>

名前	説明
[ユーザー名 (Username)] field	ユーザー名を入力します。 ユーザー名 ルールの UI 手順に従ってください。
ユーザーパスワード field	ユーザのパスワードを入力します。 パスワードルールの UI 手順に従ってください。
ユーザーパスワードの確認 field	確認のためにパスワードを再入力します。
権限 ドロップダウンリスト	[バーチャルアカウント (Virtual Account)]ドロップ ダウン リストから、 権限 ドロップダウン リストか ら、適切なロールを選択します： 管理者フルアクセスとコントロール。 演算子制限された操作アクセス。 ReadOnly : 表示専用アクセス。
パスワードの変更が必須 オプション ボタンを選択 します	選択 有効 ユーザーにより初回ログイン時にパスワー ドを変更する必要があります。 選択 ディセーブル ユーザーにより初期パスワード を保持できます。
VMediaアクセス オプション ボタンを選択します	選択 有効 ユーザーが仮想メディア機能（例：ISO ファイルのマウント）を利用できるようにします。 選択 ディセーブル 仮想メディア機能に対するユー ザーのアクセスを制限します。

ステップ5 登録手続きを開始するには、**ユーザーの追加**。

ユーザの編集

手順

ステップ1 [Navigation] ペインから、[管理]>[ユーザー管理]をクリックします。

ステップ2 ユーザー管理 タブを選択します。

ステップ3 ユーザーを編集するには、**編集** アイコン（編集するユーザーレイヤに該当する）をクリックします。
ユーザーの編集 ウィンドウが表示されます。

ステップ4 次に **ユーザーの編集** ウィンドウで次のプロパティを更新します。

名前	説明
アカウントステータス オプション ボタンを選択します	<p>[All Blocks] ドロップダウン メニューを選択してレポートを選択し、結果の生成と表示を行います。有効 ラジオ ボタンを選択し、アカウントを即時にアクティベートします。</p> <p>[All Blocks] ドロップダウン メニューを選択してレポートを選択し、結果の生成と表示を行います。ディセーブル [無効化 (Disabled)] ラジオ ボタンを選択し、アクティベーション無しでアカウントを作成します。</p>
[ユーザー名 (Username)] field	<p>ユーザー名を入力します。</p> <p>ユーザー名 ルールの UI 手順に従ってください。</p>
ユーザーパスワード field	<p>ユーザのパスワードを入力します。</p> <p>パスワード ルールの UI 手順に従ってください。</p>
ユーザーパスワードの確認 field	<p>確認のためにパスワードを再入力します。</p>
権限 ドロップダウンリスト	<p>[バーチャルアカウント (Virtual Account)] ドロップダウン リストから、権限 ドロップダウン リストから、適切なロールを選択します：</p> <p>管理者フル アクセスとコントロール。</p> <p>演算子制限された操作アクセス。</p> <p>ReadOnly：表示専用アクセス。</p>
パスワードの変更が必須 オプション ボタンを選択します	<p>選択 有効 ユーザーにより初回ログイン時にパスワードを変更する必要があります。</p> <p>選択 ディセーブル ユーザーにより初期パスワードを保持できます。</p>
VMediaアクセス オプション ボタンを選択します	<p>選択 有効 ユーザーが仮想メディア機能（例：ISO ファイルのマウント）を利用できるようにします。</p> <p>選択 ディセーブル 仮想メディア機能に対するユーザーのアクセスを制限します。</p>

ステップ 5 [保存 (Save)] を [Save]。

ユーザーの有効化または無効化

手順

ステップ 1 [Navigation] ペインから、[管理]>[ユーザー管理]をクリックします。

ステップ 2 ユーザー管理 タブを選択します。

ステップ 3 ユーザーを有効または無効にするには、有効または無効にするユーザーの行に対応するチェックボックスをオンにします。

チェックボックスをオンにする時、追加オプションを含む新しいヘッダー行がテーブルの上に現れます。

ステップ 4 登録手続きを開始するには、**Enable/無効**。

アカウント ポリシー設定を管理

手順

ステップ 1 [Navigation] ペインから、[管理]>[ユーザー管理]をクリックします。

ステップ 2 ユーザー管理 タブを選択します。

ステップ 3 登録手続きを開始するには、**アカウントポリシー設定**。

アカウントポリシー設定 ウィンドウが表示されます。

ステップ 4 次にアカウントポリシー設定 ウィンドウで次のプロパティを更新します。

名前	説明
ログイン失敗回数の上限 field	0 から 65535 までの値を入力してください。
ユーザーのロック解除方法 オプション ボタンを選択します	次のオプションのいずれかを選択します。 [Manual]以下の [Manual] オプション ボタンを選択し、ロック解除のために手動による介入を要求します。 タイムアウト後に自動以下のタイムアウト後に自動ラジオボタンを使用して、指定したタイムアウト後に自動的にロックを解除できます。
タイムアウト時間(秒) field	条件 タイムアウト後に自動 が選択されている場合は、次に秒数を入力します。タイムアウト時間(秒) field.

ステップ5 [保存 (Save)] を [Save]。

ユーザの削除

手順

ステップ1 [Navigation] ペインから、[管理]>[ユーザー管理]をクリックします。

ステップ2 ユーザー管理 タブを選択します。

ステップ3 ユーザーを削除するには、削除するユーザーの行に対応するチェック ボックスをオンにします。

チェック ボックスをオンにする時、追加オプションを含む新しいヘッダー行がテーブルの上に現れます。

ステップ4 [削除 (Delete)] を **削除 (Delete)** の「Configuring RAID Levels」の章を参照してください。

ステップ5 または、削除するユーザー行に対して削除アイコンをクリックすることもできます。

パスワード設定の管理

手順

ステップ1 [Navigation] ペインから、[管理]>[ユーザー管理]をクリックします。

ステップ2 ユーザー管理 タブを選択します。

ステップ3 [パスワード設定]の下で、次のプロパティを更新します。

名前	説明
複雑度 ドロップダウンリスト	<p>複雑度 ドロップダウンリストで、ユーザーに必要なパスワードの複雑度レベルを定義します。次のオプションを使用できます。</p> <p>ディセーブル：パスワードの複雑さに関する制限は適用されません。</p> <p>低：基本的な複雑さの要件（文字と数字の両方を含めるなど）を満たすパスワードを要求します。</p> <p>中：文字、数字、特殊文字の組み合わせなど、より厳しい複雑さのルールを満たすようにパスワードを要求します。</p> <p>高：大文字と小文字、数字、特殊文字の使用、最小長など、パスワードの最も厳格なルールを適用します。</p> <p>(注) IPMI 2.0 の制限により、20 バイトを超えるパスワードは使用できません。</p>
[パスワード履歴 (Password History)] ドロップダウンリスト	<p>[パスワード履歴 (Password History)] ドロップダウンリストで、各ユーザーに保存する以前のパスワードの数を指定します。これにより、ユーザが最近使用したパスワードを再使用することを防止できます。次のオプションを使用できます。</p> <p>0：パスワード履歴は適用されません。ユーザーは以前のパスワードを再利用できます。</p> <p>1：システムは最後の 1 つのパスワードを記憶します。ユーザーは最新のパスワードを再利用できません。</p> <p>2：システムは最後の 2 つのパスワードを記憶します。</p> <p>3：システムは最後の 3 つのパスワードを記憶します。</p> <p>4：システムは最後の 4 つのパスワードを記憶します。</p> <p>5：システムは最後の 5 つのパスワードを記憶するため、最高レベルのパスワード再利用防止が提供されます。</p>

LDAP 設定

LDAP 認証のイネーブル化

リスト Cisco BMC 2.0では、SSH、Redfish、Web サーバ、およびホスト コンソール インターフェイスにより、LDAP ディレクトリに対する認証が許可されます。ただし、IPMI インターフェイスは、セッションのセットアップ時にクリア テキストのパスワードを要求するため、LDAP に対して認証できません。PAM ベースの認証が実装されているため、LDAP ユーザーとローカルユーザーの両方で認証フローが同じになります。

LDAP ユーザー アカウントの場合、権限ロールに対応する LDAP 属性タイプは Cisco BMC 2.0 ありません。推奨される方法は、LDAP ユーザー アカウントを LDAP グループにグループ化することです。その後、Redfish と GUI を使用して、特権ロールを LDAP グループに割り当てることができます。

手順

ステップ 1 [Navigation] ペインから、[管理] > [ユーザー管理] をクリックします。

ステップ 2 LDAP タブを選択します。

ステップ 3 通常の LDAP 認証次のプロパティを更新します。

名前	説明
Enable チェックボックス	※ Enable チェックボックスをオンにして、LDAP 認証オプションをアクティブにします。
SSLを使用したセキュアLDAP チェックボックス	LDAP 通信を暗号化するには、Secure LDAP over SSL を有効にします。 このオプションを有効にする前に、CA 証明書と LDAP 証明書の両方があることを確認してください。
サービス タイプ オプション ボタンを選択します	オプション ボタンを選択して、適切なサービス タイプを選択します。 OpenLDAP : ディレクトリ サービスとして OpenLDAP を使用するには選択します。 アクティブディレクトリ Microsoft の Active Directory サービスを使用するには選択します。
サーバーURI field	サーバーの URI を入力します。
[バインド DN (Bind DN)] field	ベース識別名を入力します。

名前	説明
[バインド パスワード (Bind Password)] field	バインド DN のパスワードを入力します。
ベース DN (Base DN) field	ベース識別名を入力します。
ユーザ ID 属性 (オプション) フィールド。	ユーザーの識別の属性を入力します。
[グループ ID 属性 (Group ID Attribute)] (オプション) フィールド。	グループの識別の属性を入力します。
[SSL 証明書の管理 (Manage SSL Certificate)] リンク	詳細については、[新しい証明書の追加 (Adding a New Certificate)] クリックします。

ステップ 4 登録手続きを開始するには、設定の保存。

ロール グループの追加

グループロールは、ユーザの第1レベルの許可を決定し、必要なインターフェイスへのアクセスが許可されるかどうかを確立します。たとえば、ユーザーが Web サーバー グループにのみ属し、SSH グループに属していない場合、ユーザーは SSH にログインできません。共通のユーザー管理内にグループロールがあると、異なるアプリケーションが相互にロールを作成できます。たとえば、管理ユーザーは Web サーバーを介して新しいユーザーを作成し、Web サーバー、Redfish、IPMI、およびその他のインターフェイスにログインする機能を付与できます。

始める前に

LDAP 認証が有効になっていることを確認します。

手順

ステップ 1 [Navigation] ペインから、[管理]>[ユーザー管理]をクリックします。

ステップ 2 LDAP タブを選択します。

ステップ 3 登録手続きを開始するには、**ロールグループの追加**。

新しいロールグループの追加 ウィンドウが表示されます。

ステップ 4 次に **新しいロールグループの追加** ウィンドウで次のプロパティを更新します。

名前	説明
グループ名 (Group Name) field	システム内で識別するために、役割グループの名前を入力します。

名前	説明
グループ権限 field	ドロップダウンリストからグループに適切なレベルのアクセスを選択します： 管理者フルアクセスとコントロール。 演算子制限された操作アクセス。 ReadOnly ：表示専用アクセス。

ステップ5 次にクリックします 追加 (Add)。

Active Directory

値は、Cisco BMC 2.0 は、ユーザー認証と承認に Active Directory を使用するように構成できます。Active Directory を使用するには、に関するユーザー ロール情報とロケール情報を保持する属性を使ってユーザーを構成します。Cisco BMC 2.0。ユーザー ロールまたはロケールにマップされている既存の LDAP 属性を使用するか、Cisco BMC 2.0 既存の LDAP 属性を使用できます。または、LDAP スキーマを変更して、属性 ID 1.3.6.1.4.1.9.287247.1 を持つ CiscoAVPair 属性などの新しいカスタム属性を追加できます。Active Directory スキーマ変更の詳細については、以下を参照してください。 <http://technet.microsoft.com/en-us/library/bb727064.aspx>。

Active Directory サーバーの構成

Active Directory サーバーにカスタム属性を作成するには、次の手順を活用。



(注) この例では CiscoAVPair という名前のカスタム属性を作成しますが、次のユーザー ロールとロケールにマップされた既存の LDAP 属性を使用することも Cisco BMC 2.0 できます。

手順

ステップ1 Active Directory スキーマ スナップインがインストールされていることを確認します。

ステップ2 Active Directory スキーマ スナップインを使用して、次のプロパティを持つ新しい属性を追加します。

プロパティ	値
共通名	CiscoAVPair
LDAP Display Name	CiscoAVPair
Unique X500 Object ID	1.3.6.1.4.1.9.287247.1
[説明 (Description)]	CiscoAVPair

プロパティ	値
構文	Case Sensitive String

ステップ 3 Active Directory スナップインを使用して、ユーザー クラスに CiscoAVPair 属性を追加します。

- a) 次の展開 **クラス** ノードを展開し、U を入力してユーザー クラスを選択します。
- b) [削除 属性 タブをクリックして、追加 (Add)。
- c) C を入力して CiscoAVPair 属性を選択します。
- d) 次をクリックします **[OK] をクリックします** をクリックします。

この手順により、新しい属性がユーザー クラスに関連付けられ、システム内で効果的に使用できるようになります。

ステップ 4 にアクセスできるようにするユーザーに対し、次のユーザー ロール値を CiscoAVPair 属性に追加します。
Cisco BMC 2.0:

ロール	CiscoAVPair 属性値
admin	shell:roles="admin"
user	shell:roles="user"
read-only	shell:roles="read-only"

(注)

属性への値の追加の詳細については、<http://technet.microsoft.com/en-us/library/bb727064.aspx> と呼ばれます。

次のタスク

使用 Cisco BMC 2.0 Active Directory を構成します。

ユーザ セッション

ユーザ セッションの表示

手順

ステップ 1 [Navigation] ペインから、[管理]>[ユーザー管理]をクリックします。

ステップ 2 セッション管理 タブを選択します。

ステップ 3 次のプロパティを表示することができます：

名前	説明
セッション ID column	トラッキングおよび管理の目的で、各アクティブな Web ユーザーセッションに割り当てられる一意の識別子。
セッション タイプ column	次のように、使用されているセッションのタイプを示します。 Redfish , Web UI または CLI 。
[ユーザ ID (User ID)] column	ユーザーに割り当てられる数値識別子。 [ユーザー名 (Username)]。
[ユーザー名 (Username)] column	サーバー ログイン セッションに関連付けられているアカウント名。
IP アドレス column	セッション中にサーバーにアクセスするデバイスのネットワークアドレス。
権限 column	セッションに割り当てられるアクセスまたは権限のレベルを指定します。たとえば、 管理者 , 演算子 または ReadOnly 。

セッションの切断

手順

ステップ 1 [Navigation] ペインから、[管理]>[ユーザー管理]をクリックします。

ステップ 2 セッション管理 タブを選択します。

ステップ 3 1つのセッションを削除することも、複数のセッションをまとめて削除することもできます。

- セッションを削除するには、削除するセッション行の削除アイコンをクリックします。
- 複数のセッションを削除するには、削除するセッションの行に対応するチェック ボックスをオンにします。

チェック ボックスをオンにする時、追加オプションを含む新しいヘッダー行がテーブルの上に現れます。

[削除 (Delete)] を **削除 (Delete)** 。



第 5 章

リモート プレゼンスの管理

- [仮想メディアの設定 \(65 ページ\)](#)
- [仮想 KVM コンソール \(66 ページ\)](#)

仮想メディアの設定

仮想メディアの構成

手順

ステップ 1 [Navigation] ペインから、[コンピューティング]>[リモート管理]をクリックします。

ステップ 2 [仮想メディア (Virtual media)] タブを選択します。

ステップ 3 次のプロパティを更新します。

名前	説明
イメージリダイレクトのための仮想メディアの有効化 トグル ボタン	リモート対応メディアを有効または無効にできます。
再試行間隔 (Retry Interval) フィールド	リモート対応メディア操作の再試行の時間間隔を指定します。
再試行回数 (Retry Count) フィールド	リモート対応メディア操作に許可される再試行の最大数を示します。
Webブラウザからイメージを読み込む	
ファイルの追加 ボタン	ローカルシステムから対応するスロット (スロット 1 またはスロット 2) に、ファイル (ISO イメージやリモート対応ディスクなど) を選択してアップロードできます。

名前	説明
開始 (Start) ボタン	対応するスロットにアップロードされたファイルのリモート対応メディア操作を開始できます。
外部サーバーからイメージを読み込む	
ファイルの追加 ボタン	外部サーバから対応するスロット (スロット 1 またはスロット 2) にファイル (ISO イメージやリモート対応ディスクなど) を指定してアップロードできます。
開始 (Start) ボタン	外部サーバから対応するスロットにアップロードされたファイルのリモート対応メディア操作を開始できます。

仮想 KVM コンソール

vKVM コンソールは、サーバへのキーボード、ビデオ、Cisco BMC 2.0 マウス (KVM) の直接接続をエミュレートするアクセス可能なインターフェイスです。遠隔地のサーバから接続して制御し、この vKVM セッション中にアクセスできる仮想ドライブに物理ロケーションをマッピングすることができます。

Cisco KVM コンソールを使用する主な利点は次のとおりです。

- Cisco KVM コンソールは KVM、SOL、および vMedia への接続を提供しますが、Avocent KVM は KVM および vMedia への接続のみを提供します。
- KVM コンソールでは、vMedia 接続が KVM 起動マネージャで確立され、すべてのユーザーが使用できます。
- KVM コンソールには、ゲストからホストにテキストを貼り付ける際に、サポートされていない文字の高度な文字置換オプションが用意されています。
- KVM コンソールには、Cisco BMC 2.0 に vMedia マッピングを保存する機能があります。

サーバに物理的に接続された CD/DVD ドライブまたはフロッピー ドライブを使用する代わりに、vKVM コンソールは仮想メディアを使用します。これは、仮想 CD/DVD ドライブまたはフロッピー ドライブにマップされる実際のディスク ドライブまたはディスク イメージファイルです。次のいずれでも仮想ドライブにマップできます。

- PXE
- [HDD]
- CD
- USB

vKVM コンソールを使用してサーバに OS をインストールできます。

表 26: コンソール メニュー

メニュー項目	説明
KVM	現用系のコンソールとして KVM (Keyboard Video and Mouse) を選択します。
SOL	現用系のコンソールとして SOL (Serial Over LAN) を選択します。 (注) SOL が非アクティブな場合、SOL は表示されません。代わりに、[SQL を有効化 (Activate SOL)] が表示されます。
SOL を有効化	ユーザー名とパスワードを使用して SOL セッションにログインできます。 (注) [SQL を有効化 (Activate SOL)] オプションは、何らかの理由で SOL セッションがアクティブでない場合にのみ表示されます。

表 27: [電源メニュー (Power Menu)]

メニュー項目	説明
電源オフ (Power Off)	仮想コンソール セッションからシステムの電源をオフにします。 (注) このオプションは、システムの電源がオンの場合に有効で、システムの電源がオフの場合は無効です。
電源オン	システムの電源を入れます。 (注) このオプションは、システムの電源がオンになっている場合は無効で、システムの電源がオフになっている場合に有効です。

メニュー項目	説明
[電源の再投入 (Power Cycle)]	システムの電源をオフにしてから、再度オンにします。 (注) このオプションは、システムの電源がオンの場合に有効で、システムの電源がオフの場合は無効です。
Power Down	システム電源はオフにします。 (注) このオプションは、システムの電源がオンの場合に有効で、システムの電源がオフの場合は無効です。

表 28: [起動デバイスメニュー (Boot Device Menu)]

メニュー項目	説明
なし (None)	ブートデバイスが選択されていません。
PXE	ブートデバイスとして PXE (Preboot Execution Environment) を選択します。
[HDD]	ハードディスクドライブ (HDD) をブートデバイスとして選択します。
CD	ブートデバイスとして CD/DVD ドライブを選択します。
BiosSetup	ブートオプションとして [BIOS セットアップ (BIOS Setup)] を選択します。
USB	ブートデバイスとして CDROM ドライブを選択します。

表 29: [仮想メディアメニュー (Virtual Media Menu)]

メニュー項目	説明
イメージのマッピング	ローカルイメージ (ISOファイルなど) をリモート対応メディアにマッピングできます。
イメージの取り出し	リモート対応メディアから現在マッピングされているローカルイメージのマッピングを解除またはイジェクトできます。

メニュー項目	説明
外部イメージのマッピング	外部サーバにあるイメージ ファイルをリモート対応メディアにマッピングできます。
外部イメージの取り出し	現在マッピングされている外部イメージのマッピングを解除またはリモート対応メディアからイジェクトできます。

KVM コンソールの起動



- (注) 読み取り/書き込み機能を備えているのは最初の KVM セッションのみです。他のすべての同時セッションは読み取り専用です。

手順

- ステップ 1 次のいずれかの方法から KVM を起動できます。
- ステップ 2 [削除 KVM の起動 [メニュー (Menu)] バーアイコンをクリックします。
- ステップ 3 または、[計算 (Compute)] > [リモート管理 (Remote Management)] の順に選択します。 > > [削除 KVM の起動] ボタンを押します。

仮想 KVM の設定

手順

- ステップ 1 [Navigation] ペインから、[コンピューティング] > [リモート管理] をクリックします。
- ステップ 2 [All Blocks] ドロップダウン メニューを選択してレポートを選択し、結果の生成と表示を行います。 **KVM** タブに表示されるフィールドとアイコンについて説明します。
- ステップ 3 次のプロパティを更新できます。

名前	説明
KVM ゲスト オペレーティング システムに対して KVM を有効にします トグル ボタン	仮想 KVM を有効または無効にできます。

名前	説明
KVMポート値(数値) field	KVM (キーボード、ビデオ、マウス) 通信に使用するポート番号を指定します。この値は数値として入力する必要があり、システム上の KVM アクセス用に構成されたポートに対応している必要があります。 [保存 (Save)] を [Save] クリックして変更を保存します。
KVMセッションタイムアウト field	アクティブな KVM セッションが自動的にタイムアウトするまでの非アクティブ時間を定義します。これにより、指定の時間の経過後に未使用の接続が切断されるため、セッションのセキュリティが確保されます。 [保存 (Save)] を [Save] クリックして変更を保存します。

仮想 KVM の無効化

手順

- ステップ 1 [Navigation] ペインから、[コンピューティング]>[リモート管理]をクリックします。
- ステップ 2 [All Blocks] ドロップダウンメニューを選択してレポートを選択し、結果の生成と表示を行います。 **KVM**。
- ステップ 3 [削除 [KVMを有効にすると、ゲストオペレーティングシステムに対して KVM を有効にする (Enabling KVM makes to the guest operating system)] トグル ボタンをクリックし、KVM を有効または無効にします。
- 有効にすると、ゲストオペレーティングシステムへのアクセスが許可されます。



第 6 章

ネットワーク関連の設定

- [ネットワーク設定内の構成内の Cisco BMC 2.0](#) (71 ページ)
- [Network Time Protocol の設定](#) (76 ページ)

ネットワーク設定内の構成内の Cisco BMC 2.0

Cisco BMC 2.0 は、Web GUI、Redfish、IPMI コマンドなどのさまざまなインターフェイスを提供し、BMC ネットワークの包括的な管理を容易にします。ネットワーク構成には、IP アドレス、IP アドレス送信元、ゲートウェイの構成などのタスクが含まれます。

基本的なネットワーク構成機能は次のとおりです：

- IP アドレス送信元
- IP アドレス
- [ゲートウェイ (Gateways)]
- サブネット マスク

ネットワーク設定の表示または構成



(注) 共有 NIC (eth1) は、X710 OCP カードに関連付けられます。接続とパフォーマンスを最適化するためにネットワークインターフェイスを設定するときに、この構成が考慮されていることを確認します。

管理トラフィックに OCP (eth1) を使用する場合、NCSI サポートは OCP カードのポート 1 のみ使用できます。

手順

ステップ1 [Navigation] ペインから、管理 > ネットワーキングをクリックします。

ステップ2 [ネットワーク設定] タブを選択します。

ステップ3 [ネットワーク設定 (Network Settings)] で、次のプロパティを更新します：

[名前 (Name)]	説明
ホストネーム (Hostname) field	BMC の完全修飾ドメイン名 (FQDN) を指定します。 編集ボタンをクリックして、ドメイン名を更新します。
ドメイン名を使用 トグル ボタン	ネットワーク通信にドメイン名を使用するオプションを有効または無効にします。
DNSサーバーを使用 トグル ボタン	ホスト名を IP アドレスに解決するために DNS サーバーを使用するオプションを有効または無効にします。
NTPサーバーを使用 トグル ボタン	ネットワーク タイム プロトコル サーバを使用して BMC のクロックを同期するオプションを有効または無効にします。
共有NIC (eth1)を使用 トグル ボタン	ネットワーク接続に共有ネットワークインターフェイス カード (NIC) eth1 を使用するオプションを有効または無効にします。

ステップ4 eth0/ehl1では、次のプロパティを表示できます。

[名前 (Name)]	説明
リンクステータス field	ネットワークリンクの現在のステータスを示し、アクティブ (LinkUp) か非アクティブかを示します。
速度 (Mbps) field	ネットワーク接続の現在の速度をメガビット/秒 (Mbps) で表示します。
[FQDN] field	インターフェイスに割り当てる完全修飾ドメイン名 (FQDN) を指定します。
MAC アドレス field	ネットワークインターフェイスに割り当てられた一意の Media Access Control (MAC) アドレスを表示します。

ステップ5 ビジネスインサイトの [IPv4 アドレスの表示または追加 \(73 ページ\)](#) IPv4 アドレスと [IPv6 アドレスの表示または追加 \(74 ページ\)](#) IPv6 アドレスを更新します。

ステップ6 登録手続きを開始するには、[設定の保存](#)。

IPv4 アドレスの表示または追加

手順

ステップ1 [Navigation] ペインから、[管理 > ネットワーキング](#)をクリックします。

ステップ2 [ネットワーク設定] タブを選択します。

ステップ3 通常の IPv4 次のプロパティを更新します。

名前	説明
現在のアドレス発信元	現在の IPv4 アドレス設定を指定します。
DHCP オプション ボタンを選択します	これにより、自動 IP アドレス割り当てに Dynamic Host Configuration Protocol (DHCP) を選択することができます。
[静的 (Static)] オプション ボタンを選択します	これにより、静的 IP 構成を選択できます。この場合、IP アドレス、ゲートウェイ、およびサブネットマスクの詳細を手動で入力する必要があります。 [静的 (Static)] を有効にした時にフィールドは、有効になります。
IP アドレス (IP Address) field	ネットワーク上でデバイスを一意に識別する、デバイスに割り当てられたインターネット プロトコル (IP) アドレスを指定します。
[Gateway] field	ネットワーク ゲートウェイの IP アドレスを入力します。ネットワーク ゲートウェイは、ローカルネットワークと他のネットワークまたはインターネットとの間でトラフィックを渡すアクセスポイントまたはルータとして機能します。
サブネット マスク field	IP アドレスのどの部分がネットワークを参照し、どの部分がデバイスを参照するかを指定して、ネットワーク アドレスの範囲を入力します。

IPv6 アドレスの表示または追加

手順

ステップ 1 [Navigation] ペインから、管理 > ネットワーキングをクリックします。

ステップ 2 [ネットワーク設定] タブを選択します。

ステップ 3 通常の IPv6 次のプロパティを更新します。

名前	説明
現在のアドレス発信元	現在の IPv6 アドレス設定を指定します。
DHCPv6/SLAAC オプション ボタンを選択します	Dynamic Host Configuration Protocol (DHCP) または Stateless Address Autoconfiguration (ステートレス アドレス自動設定) による自動 IPv6 アドレス構成を有効にできます。
[静的 (Static)] オプション ボタンを選択します	静的 IP 構成を選択できます。この場合、IP アドレスとプレフィックス長の詳細を手動で入力する必要があります。 [静的 (Static)] を有効にした時にフィールドは、有効になります。
IP アドレス (IP Address) field	ネットワーク上でデバイスを一意に識別する、デバイスに割り当てられたインターネット プロトコル (IP) アドレスを指定します。
プレフィックス長 field	プレフィックス長を指定して、IPv6 アドレスのネットワーク部分を定義します。これにより、サブネットのサイズが決まります。
IPv6 デフォルトゲートウェイ field	編集アイコンをクリックしてダイアログボックスを開き、トラフィックをローカルネットワークの外部にルーティングするためのデフォルトゲートウェイの IPv6 アドレスを入力します。
リンクローカルアドレス field	ローカル ネットワーク セグメント内の通信に使用される、自動的に割り当てられるリンクローカル IPv6 アドレスを表示します。編集できません。
SLAAC アドレス field	自律デバイス通信に割り当てられた、自動的に設定された SLAAC IPv6 アドレスを表示します。編集できません。

静的 DNS IP アドレスの表示、追加、または削除

手順

ステップ 1 [Navigation] ペインから、**管理 > ネットワーキング** をクリックします。

ステップ 2 [ネットワーク設定] タブを選択します。

ステップ 3 通常の静的 DNS の場合、**IP アドレスの追加**。

IP アドレスの追加 ウィンドウが表示されます。

ステップ 4 次に **IP アドレスの追加** ウィンドウで、次のプロパティを更新します。

名前	説明
静的 DNS field	DHCP が無効の場合にドメイン名解決に使用する静的 DNS サーバー アドレスを入力します。

ステップ 5 次をクリックします **追加 (Add)**。

ドメイン名の表示、追加、または削除

始める前に



(注) 最大1台のドメイン名サーバーのみを指定できます。

手順

ステップ 1 [Navigation] ペインから、**管理 > ネットワーキング** をクリックします。

ステップ 2 [ネットワーク設定] タブを選択します。

ステップ 3 通常のドメイン名の場合、**追加 (Add)**。

ドメインアドレスの追加 ウィンドウが表示されます。

ステップ 4 次に [ドメインの追加 (Add Domain)] ウィンドウで、次のプロパティを更新します。

名前	説明
ドメイン名 field	適切なアドレッシングとアクセスのために、ネットワークまたはリソースを識別するドメイン名を入力します。

ステップ5 次をクリックします **追加 (Add)**。

ステップ6 (任意) ドメイン名を削除するには、削除する行に対応する削除アイコンをクリックします。

Network Time Protocol の設定

デフォルトでは、Cisco BMC 2.0 リセットされると、ホストと時刻が同期されます。NTP サービスを使用して、次を構成して、Cisco BMC 2.0 NTP サーバと時刻を同期します。デフォルトでは、NTP サーバはCisco BMC 2.0 動作しません。少なくとも1台、最大4台の、NTP サーバまたは時刻源サーバとして動作するサーバのIP/DNSアドレスを指定し、NTP サービスを有効にして設定する必要があります。NTP サービスを有効にすると、Cisco BMC 2.0 構成されたNTP サーバと時刻を同期します。NTP サービスは以下でのみ変更できます Cisco BMC 2.0。



(注) NTP サービスを有効にするには、DNS アドレスではなく、サーバの IP アドレスを指定することを推奨します。

Network Time Protocol 設定の指定



(注) NTP を設定すると、IPMI の Set SEL time コマンドはディセーブルになります。

手順

ステップ1 [Navigation] ペインから、**管理 > ネットワーキング**をクリックします。

ステップ2 [NTP 設定] タブを選択します。

ステップ3 リスト **設定の実施** エリアで、次のオプションから選択します。

- 手動
- NTP

ステップ4 APIC と CSSM 間の後続の通信では、[Manual]次のプロパティを更新します。

名前	説明
Date YYYY-MM-DD field	YYYY-MM-DD 形式で入力します。
24-hour time (UTC) HH:MM field	HH:MM フォーマットで時間を入力します。

ステップ5 APIC と CSSM 間の後続の通信では、**NTP**次のプロパティを更新します。

名前	説明
サーバ 1 field	最初の NTP サーバーを指定します。
サーバ 2 field	2 番目の NTP サーバーを指定します。
サーバ 3 field	3 番目の NTP サーバーを指定します。

ステップ 6 登録手続きを開始するには、**設定の保存**。



第 7 章

ストレージ設定の管理

- [コントローラの管理 \(79 ページ\)](#)
- [NVMe ドライブの管理 \(83 ページ\)](#)

コントローラの管理

変更管理チケット情報の表示

手順

ステップ 1 [Navigation] ペインから、[ストレージ] > [MSTOR- RAID] をクリックします。

ステップ 2 [コントローラ情報 (Controller Info)] タブを選択します。

ステップ 3 全般 領域の下で、領域で、次のプロパティを更新します。

名前	説明
製品名 (Product Name)	製品の名前を表示します。
[製品 ID (Product ID)] フィールド	一意の製品識別子を表示します。
ヘルス フィールド	製品の動作ステータスまたは正常性を示します。
製造業者 フィールド	製造元の名前。
シリアル番号 (Serial Number) フィールド	製品のシリアル番号を表示します。
ファームウェアバージョン (Firmware Version) フィールド	製品にインストールされているファームウェアのバージョンを示します。
Device ID	deviceId : デバイスの固有識別子。

名前	説明
サブ デバイス ID フィールド	製品に関連付けられたサブデバイス識別子を示します。
Vendor ID フィールド	ベンダーの一意の識別子を表示します。
サブベンダー ID フィールド	製品に関連付けられたサブベンダー識別子を示します。
サポートされる RAID レベル フィールド	製品がサポートする RAID レベルを示します。
速度(Gb/s) フィールド	データ転送速度 (ギガビット/秒) を示します。

ステップ 4 [物理ドライブ数 (Physical Drive Count)] 領域で、次のプロパティを更新します。

名前	説明
存在するディスク数 フィールド	現在存在するディスクの合計数を表示します。
重大なディスク数 フィールド	クリティカル状態のディスクの数を示します。
障害が発生したディスクの数 フィールド	障害が発生したディスクの合計数を表示します。

ステップ 5 [仮想ドライブ数 (Virtual Drive Count)] 領域で、次のプロパティを更新します。

名前	説明
[仮想ドライブ数 (Virtual Drive Count)] フィールド	現在設定されているリモート対応ドライブの合計数を表示します。
オフラインドライブ数 フィールド	現在オフラインであるドライブの数を表示します。

NVMe 物理ドライブ情報の表示

手順

ステップ 1 [Navigation] ペインから、[ストレージ]>[MSTOR- RAID]をクリックします。

ステップ 2 [物理ドライブ情報 (Physical Drive Info)] タブを選択します。

ステップ 3 各ドライブの次のプロパティを表示できます。

名前	説明
Id column	物理ドライブの一意の識別子を表示します。

名前	説明
メディアタイプ column	物理ドライブで使用されているメディアのタイプを示します。
ヘルス column	物理ドライブの現在の正常性ステータスを表示します。
状態 column	物理ドライブの動作状態を示します。
容量(GB) column	物理ドライブの合計ストレージ容量をギガバイト単位で表示します。
モデル (Model) column	物理ドライブのモデル名または番号が表示されます。
改訂 column	物理ドライブのファームウェアまたは改訂バージョンを示します。
ドライブの詳細	
[名前 (Name)] field	物理ドライブに割り当てられた名前が表示されます。
ヘルス field	物理ドライブの現在の正常性ステータスを表示します。
状態 field	物理ドライブの動作状態を示します。
製造業者 field	物理ドライブの製造元の名前を表示します。
シリアル番号 (Serial Number) field	物理ドライブに割り当てられた一意のシリアル番号を示します。
モデル (Model) field	物理ドライブのモデル名または番号が表示されます。
メディアタイプ field	物理ドライブで使用されているメディアのタイプを示します。
改訂 field	物理ドライブのファームウェアまたは改訂バージョンを示します。
容量(GB) field	物理ドライブの合計ストレージ容量をギガバイト単位で表示します。
ブロックサイズ(バイト) field	物理ディスクのブロックサイズ (バイト単位) を示します。

名前	説明
ネゴシエートされた速度(Gbs) field	物理ドライブとネゴシエートされたデータ転送速度 (ギガビット/秒) を示します。

仮想ドライブ情報の表示

手順

ステップ1 [Navigation] ペインから、[ストレージ]> [MSTOR- RAID]をクリックします。

ステップ2 **Virtual Drive Info** タブを選択します。

ステップ3 次のプロパティを表示することができます：

名前	説明
ID column	仮想ドライブに割り当てられた番を示します。詳細をクリックして、ドライブに関する詳細を表示します。
[名前 (Name)] column	仮想ドライブの名前を表示します。
ヘルス column	ドライブの現在の正常性ステータスを表示します。
サイズ (GB) column	仮想ドライブのストレージ容量 (ギガバイト単位) を表示します。
RAID レベル column	仮想ドライブの RAID レベルを表示します。可能な RAID レベルは次を含みます。 <ul style="list-style-type: none"> • [Raid 0] : 単純なストライピング。 • [Raid 1] : 単純なミラーリング。 • [Raid 5] : パリティ付きストライピング。 • [Raid 6] : 2つのパリティ ドライブによるストライピング。 • [Raid 10] : スパンされたミラーリング。 • [Raid 50] : パリティ付きストライピング。 • [Raid 60] : 2つのパリティ ドライブによるスパンされたストライピング。 • [Raid 00] : スパンされたストライピング。

名前	説明
ブートドライブ column	仮想ドライブがブートドライブとして指定されているかどうかを示します。

NVMe ドライブの管理

NVME サブシステム情報の表示

手順

ステップ 1 [Navigation] ペインから、ストレージ > NVMe 情報をクリックします。

ステップ 2 NVMe MIサブシステム タブを選択します。

ステップ 3 次の [NVMe コントローラの選択 (Select NVMe Controllers)] ドロップダウン リストから、該当する言語を選択します。

ステップ 4 次の [サブシステム情報 (SubSystem Information)] タブを選択し、以下のプロパティを表示します。

名前	説明
メジャーバージョン列	NVMe サブシステムのメジャーバージョンを示します。
マイナーバージョン列	NVMe サブシステムのマイナーバージョンを示します。
ポート数 列	NVMe サブシステムで使用可能なポートの合計数を表示します。

ステップ 5 次の [ポート情報 (Port Information)] タブを選択し、以下のプロパティを表示します。

名前	説明
[ポートタイプ (Port Type)] 列	NVMe サブシステムで使用されるポートのタイプを示します。
[現在のリンク速度 (Current Link Speed)] 列	リンクの現在のデータ転送速度を表示します。
[最大リンク幅 (Max Link Width)] 列	ポートでサポートされる最大リンク幅を表示します。

名前	説明
[最大 MCTP 転送ユニットサイズ (Max MCTP Trans Unit Size)] 列	ポートでサポートされる Message Control and Transport Protocol (MCTP) トランザクションユニットの最大サイズを示します。
[最大ペイロード サイズ (Max Payload Size)] 列	ポートが処理できる最大ペイロードサイズを示します。
[ネゴシエートされたリンク幅 (Negotiated Link Width)] 列	ポートの現在ネゴシエートされたリンク幅を示します。
[ポート番号 (Port No)] 列	ポートに割り当てられた固有識別子または番号を表示します。
[ポート ステータス (Port Status)] 列	ポートの現在の動作ステータスを示します (例: [有効 (Enabled)]、[無効 (Disabled)])。
[サポートされるリンク速度 (Supported Link Speeds)] 列	ポートでサポートされているリンク速度の範囲を一覧表示します。

名前	説明
[ポート タイプ (Port Type)] 列	NVMe サブシステムで使用されるポートのタイプを示します。
[現在のアドレス (Current Address)] 列	サブシステム内のポートの現在のアドレスを表示します。
[エンドポイントのアドレス (EndPoint Address)] 列	ポートに関連付けられたエンドポイントのアドレスを表示します。
[最大エンドポイント周波数 (Max EndPoint Frequency)] 列	エンドポイントでサポートされる最大周波数を示します。
[最大周波数 (Max Frequency)] 列	ポートでサポートされている最大周波数が表示されます。
[最大 MCTP 転送ユニットサイズ (Max MCTP Trans Unit Size)] 列	ポートでサポートされる Message Control and Transport Protocol (MCTP) トランザクションユニットの最大サイズを示します。
[NVMe 基本管理コマンド (NVMe Basic Management Command)] 列	NVMe 基本管理コマンドがポートでサポートされているかどうかを示します。
[ポート番号 (Port No)] 列	ポートに割り当てられた固有識別子または番号を表示します。

名前	説明
[ポート ステータス (Port Status)] 列	ポートの現在の動作ステータスを示します (例: [有効 (Enabled)]、[無効 (Disabled)])。

ステップ 6 次の [サブシステム健全性ステータスのポーリング (SubSystem Health Status Poll)] タブを選択し、以下のプロパティを表示します。

名前	説明
[ドライブ機能 (Drive Functional)] 列	ドライブが正しく機能し、動作しているかどうかを示します。
[PDLU] 列	システムの電源切断論理ユニット (PDLU) 状態を表示します。
[合成温度 (Composite Temperature)] 列	複数のコンポーネントからのデータを組み合わせた、NVMe サブシステムの全体的な温度を示します。
[ポート 0 PCIe リンクアクティブ (Port0 PCIe LinkActive)] 列	ポート 0 の PCIe リンクがアクティブで動作しているかどうかを示します。
[ポート 1 PCIe リンク アクティブ (Port1 PCIe LinkActive)] 列	ポート 1 の PCIe リンクがアクティブで動作しているかどうかを示します。
[リセットは不要 (Reset Not Required)] 列	サブシステムが安定した状態にあり、リセットの必要がないかどうかを指定します。

表 30: 複合コントローラ ステータス

名前	説明
[使用可能なスペア (Available Spare)] フィールド	NVMe サブシステムに利用可能なスペア容量があるかどうかを示します。
[合成温度の変化 (Composite Temperature Change)] フィールド	サブシステムのコンポジット温度に変化があるかどうかを示します。
[コントローラ有効化の変更が発生 (Controller Enable Change Occurred)] フィールド	コントローラの有効化状態に変更が生じたかどうかを示します。
[コントローラの致命的ステータス (Controller Fatal Status)] フィールド	コントローラで致命的なエラーが発生したかどうかを示します。
[コントローラ ステータスの変更 (Controller Status Change)] フィールド	コントローラのステータスが変更されたかどうかを示します。

名前	説明
[重大な警告 (Critical Warnings)] フィールド	サブシステムに関して重大な警告が発行されているかどうかを示します。
[NVMe サブシステムのリセットの発生 (NVMe SubSystem Reset Occurred)] フィールド	NVMe サブシステムのリセットが発生したかどうかを示します。
[名前空間属性の変化 (Name Space Attribute Change)] フィールド	名前空間属性が変更されたかどうかを示します。
[使用率 (Percentage Used)] フィールド	使用されるドライブの容量の割合が変更されたかどうかを示します。
[準備完了 (Ready)] フィールド	NVMe サブシステムの準備が整い、動作しているかどうかを示します。
[シャットダウンステータス (Shut Down Status)] フィールド	サブシステムが正常にシャットダウンされたか、問題があるかどうかを示します。
[ファームウェアがアクティブ (Firmware Activated)] フィールド	サブシステムで新しいファームウェアバージョンがアクティブになっているかどうかを示します。

表 31 : NVMe Smart 重大警告

名前	説明
[読み取り専用メディア (Media In ReadOnly)] 列	メディアが読み取り専用状態になっているかどうかを示します。この場合、書き込み操作は実行されません。
[サブシステム全体の劣化 (Over all Subsystem Degraded)] 列	サブシステム全体で、パフォーマンスまたは機能の低下が発生したかどうかを示します。
[電力バックアップの失敗 (Power Backup Failed)] 列	電源バックアップメカニズムが故障しているか、または動作していないかを示します。
[予備容量の消耗 (Spare Capacity WornOut)] 列	サブシステムの予備容量が枯渇していないか、または使用できなくなっているかどうかを示します。

NVMe のバイタル製品データ情報の表示

手順

ステップ 1 [Navigation] ペインから、ストレージ > NVMe 情報をクリックします。

ステップ 2 NVMe MI重要製品データ タブを選択します。

ステップ 3 次の [NVMe コントローラを選択 (Select NVMe Controllers)] ドロップダウンリストから、該当する言語を選択します。

ステップ 4 次の [製品情報 (Product Information)] タブを選択し、以下のプロパティを表示します。

名前	説明
IPMI バージョン 列	製品で使用されるインテリジェントプラットフォーム管理インターフェイス (IPMI) のバージョンを示します。
製造業者 列	製品のメーカーを表示します。
モデル (Model) 列	製品のモデル名または番号を示します。
製品番号 列	製造元によって製品に割り当てられた部品番号を表示します。
シリアル番号 column	製品の一意のシリアル番号を示し、ID に使用されます。

ステップ 5 次の [マルチレコード情報 (MultiRecord Information)] プロパティを表示するには、次のいずれかのタブを選択します：

表 32: NVMe マルチレコード

名前	説明
EPT ファクタ フィールド	NVMe デバイスの EPT 係数を指定します。
初期電源要件 1.8V フィールド	1.8V 向け初期電源要件を示します。
初期電源要件 12V フィールド	12V 向け初期電源要件を指定します。
初期電源要件 3.3V フィールド	初期電源要件 3.3V
初期電源要件 5V フィールド	初期電源要件 5V
最大補助電源要件 3.3V フィールド	3.3v の最大補助電源要件を表示します。
最大電源要件 1.8V フィールド	1.8v の最大電源要件を示します。

名前	説明
最大電源要件 12V フィールド	12v の最大電源要件を指定します。
最大電源要件 3.3V フィールド	3.3v の最大電源要件を表示します。
最大電源要件 5V フィールド	5v の最大電源要件を指定します。
最大熱負荷 フィールド	デバイスの最大熱負荷を示します。
レコード エリア バージョン フィールド	レコード エリアのバージョンを表示します。

表 33: NVMe PCIe ポート マルチレコード

名前	説明
MCTP サポート 列	MCTP (Management Component Transport Protocol) がポートでサポートされているかどうかを示します。
PCIe 最大リンク幅 列	PCIe ポートでサポートされる最大リンク幅を表示します。
PCIe ポート情報 列	PCIe ポートに関する詳細情報を提供します。
PCIe ポート番号 列	PCIe ポートに割り当てられた番号を示します。
PCIe レコード バージョン 列	ポートの PCIe レコードのバージョンを表示します。
PCIe のサポート内リンク速度 列	PCIe ポートでサポートされているリンク速度を一覧表示します。

NVMe ドライブ情報の表示

手順

- ステップ 1 [Navigation] ペインから、ストレージ > NVMe 情報をクリックします。
- ステップ 2 NVMe ドライブ タブを選択します。
- ステップ 3 [バーチャルアカウント (Virtual Account)] ドロップダウンリストから、NVMeコントローラ の選択 ドロップダウンリストから、該当する言語を選択します。
- ステップ 4 次のプロパティを表示することができます：

表 34: NVMe ドライブ

名前	説明
ドライブ (Drives) 列	システムで使用可能な NVMe ドライブを一覧表示します。
ヘルス (Health) 列	NVMe ドライブの健全性状況が表示されます。
キャパシティ GB (Capacity GB) 列	NVMe ドライブのストレージ容量を GB 単位で表示します。
リビジョン (Revision) 列	NVMe ドライブにインストールされているファームウェアのリビジョンを表示します。
インジケータ LED 列	NVMe ドライブのインジケータ LED が点灯または消灯しているかどうかを表示します。
ID フィールド	NVMe ドライブの一意の識別子を表示します。
[名前 (Name)] フィールド	NVMe ドライブに割り当てられた名前が表示されます。
ヘルス (Health) フィールド	NVMe ドライブのヘルスステータスを表示します。
状態 (State) フィールド	NVMe ドライブの動作状態を表示します。
製造業者 (Manufacturer) フィールド	NVMe ドライブ製造業者の名前を表示します。
シリアル番号 (Serial Number) フィールド	NVMe ドライブのシリアル番号を表示します。
モデル (Model) フィールド	NVMe ドライブのモデル名または番号を表示します。
MediaType フィールド	SSD など、NVMe ドライブのメディアタイプを表示します。
リビジョン (Revision) フィールド	NVMe ドライブのファームウェアリビジョンを表示します。
キャパシティ GB (Capacity GB) フィールド	NVMe ドライブの容量を GB 単位で表示します。
部品番号 (Part Number) フィールド	NVMe ドライブの部品番号が表示されます。
プロトコル (Protocol) フィールド	NVMe ドライブで使用されているプロトコル (NVMe など) を示します。
セキュリティに対応 フィールド	NVMe ドライブのセキュリティ機能が表示されます。

名前	説明
セキュリティが有効 (Security Enable) フィールド	NVMe ドライブのセキュリティ機能が有効か無効かを示します。

NVMe ドライブ ロケータ LED の有効化または無効化

手順

ステップ1 [Navigation] ペインから、**ストレージ > NVMe 情報** をクリックします。

ステップ2 **NVMe ドライブ** タブを選択します。

ステップ3 NVMe ドライブに対応する行を特定します。

ステップ4 [削除 インジケータ LED] トグルボタンをクリックすると、**点灯** 位置になります。

この操作により、選択したドライブの LED がアクティブになり、サーバでのその位置が強調表示されます。



第 8 章

証明書セキュリティの管理

- 証明書の詳細の表示 (91 ページ)
- 新しい証明書の追加 (92 ページ)
- 証明書を置き換えています (93 ページ)
- 証明書を削除する (93 ページ)
- 証明書署名要求を生成する (93 ページ)

証明書の詳細の表示

証明書管理により、既存の証明書ファイルと秘密キーファイルを、認証局 (CA) によって発行された代替ファイルに簡単に置き換えることができます。この機能により、サーバー証明書とクライアント証明書の両方をシームレスに展開できます。GUI では、暗号化されていない .pem 形式の証明書と秘密キーファイルを使用して証明書を更新し、秘密キーを対応する署名付き証明書と統合できます。

手順

ステップ 1 [Navigation] ペインから、[管理] > [セキュリティ管理] をクリックします。

ステップ 2 通常の [証明書の管理 (Certificate Management)] 次のプロパティを表示することができます：

名前	説明
証明書 column	証明書の名前または、識別子を表示します。
発行 : column	証明書を発行した認証または、エンティティを表示します。
発行先 column	証明書が発行された受信者または、エンティティを示します。
有効期限の開始 column	証明書の有効期間の開始日。

名前	説明
有効期限の終了日 column	証明書の有効期間の終了日。

新しい証明書の追加

手順

ステップ1 [Navigation] ペインから、[管理]>[セキュリティ管理]をクリックします。

ステップ2 通常の [証明書の管理 (Certificate Management)] の場合、新しい証明書の追加。

新しい証明書の追加 ウィンドウが表示されます。

ステップ3 次に新しい証明書の追加 ウィンドウで次のプロパティを更新します。

名前	説明
証明書タイプ ドロップダウンリスト	次のいずれかを選択します。 <ul style="list-style-type: none"> LDAP 証明書：LDAP 接続の保護と認証に使用されます。この証明書により、システムとLDAP サーバ間の暗号化された通信が保証されます。 [HTTPS 証明書 (HTTPS Certificate)]：HTTPS 経由で Web ベースの通信を保護するために使用されます。この証明書は、クライアント (ブラウザ) とサーバ間で交換されるデータを暗号化し、プライバシーとデータの完全性を確保します。
ファイルの追加 ボタン	登録手続きを開始するには、ファイルの追加 をクリックして、クライアントから証明書ファイルを参照して選択します。

ステップ4 次をクリックします 追加 (Add)。

証明書を置き換えています

手順

ステップ1 [Navigation] ペインから、[管理]>[セキュリティ管理]をクリックします。

ステップ2 証明書を置換するには、置換する行に対応する置換アイコンをクリックします。

証明書の入れ替え ウィンドウが表示されます。

ステップ3 次に 証明書の入れ替え 次のプロパティを更新します。

名前	説明
証明書タイプ field	証明書の種類は変更できません。
ファイルの追加 ボタン	登録手続きを開始するには、 ファイルの追加 をクリックして、クライアントから証明書ファイルを参照して選択します。

ステップ4 登録手続きを開始するには、 **置き換え**。

証明書を削除する

手順

ステップ1 [Navigation] ペインから、[管理]>[セキュリティ管理]をクリックします。

ステップ2 証明書の削除を削除するには、削除する行に対応する削除アイコンをクリックします。

ステップ3 [削除 (Delete)]を **削除 (Delete)** をクリックして確認します。

証明書署名要求を生成する

手順

ステップ1 [Navigation] ペインから、[管理]>[セキュリティ管理]をクリックします。

ステップ2 通常の [証明書の管理 (Certificate Management)] の場合、[CSR の生成] を選択します。

証明書署名要求 (CSR) の生成 ウィンドウが表示されます。

ステップ3 次に 証明書署名要求 (CSR) の生成 ウィンドウで次のプロパティを更新します。

名前	説明
証明書タイプ ドロップダウン リスト	ドロップダウンメニューから、次のいずれかのオプションを選択します： <ul style="list-style-type: none"> • HTTPS 証明書：Web 通信を保護するために使用します。 • LDAP 証明書：LDAP 関連の認証に使用します。
国/地域 (Country/Region) ドロップダウン リスト	ドロップダウンメニューを国または、地域から選択します。
状態 field	都道府県名を入力します。
市区町村郡 (City) field	市区町名を入力します。
会社名 (Company Name) field	会社名を入力します。
[会社単位 (Company Unit)] field	社内のユニットを入力します。
Common Name field	証明書の一般名を入力します。
[チャレンジパスワード (オプション) (Challenge password - optional)]	パスワードを入力して、証明書のセキュリティを強化します。パスワードを指定しなければ、この追加セキュリティなしで証明書を使用できます。
[連絡先担当者 (オプション) (Contact Person - optional)] フィールド field	担当者の名前を入力してください。
[電子メールアドレス (オプション) (Email Address - optional)] field	メールアドレスを入力します。
[代理名 (任意) (Alternate Name - optional)] field	スペースで区切ると、代替の名を入力できます。
[秘密キー (Private Key)] [キー ペア アルゴリズム (Key Pair Algorithm)] ドロップダウン リスト	ドロップダウンメニューから、次のいずれかを選択します： <ul style="list-style-type: none"> • EC：短いキーでより高いセキュリティを実現する楕円曲線暗号化。 • RSA：広く使用されている暗号化方式の Rivest-Shamir-Adleman アルゴリズム。

ステップ 4 証明書署名要求を作成するには、**[CSR の生成]** をクリックしてください。



第 9 章

障害とログの管理

- システム イベント ログ (97 ページ)
- POST ログ (99 ページ)
- テクニカル サポート ログ (100 ページ)

システム イベント ログ

システム イベント ログの表示

手順

- ステップ 1 [Navigation] ペインから、[システム]>[ログ]をクリックします。
- ステップ 2 システム イベント ログ タブを選択します。
- ステップ 3 次のオプションに基づいてイベント ログをフィルタ処理できます。
- 開始と終了の日付
 - 重要度に基づく：（OK、Warning、および Critical）
 - 検索フィールドを使用して検索キーワード

次のログ プロパティを表示することができます：

名前	説明
ID コラム	各ログ エントリの一意の識別子を表示します。

名前	説明
重大度 コラム	<p>ログ エントリの重要度または影響のレベルを示します。次のいずれかになります。</p> <ul style="list-style-type: none"> • [OK] をクリックします：ログ エントリが正常または成功した操作を表していることを示します。 • クリティカル：すぐに対処が必要な重大な問題があることを示します。 • 警告：モニタする必要がある潜在的な問題を示します。
日付 コラム	ログ エントリが記録された日時を表示します。
説明 コラム	ログ エントリに関する簡単な概要または詳細を提供します。
ステータス トグル ボタン	<p>llog エントリのステータスを 解決済み と 未解決 の間で切り替えます。</p> <p>各行には、その特定のログ エントリのステータスを更新するための独自のトグル ボタンがあります。</p>
[エクスポート (Export)] アイコン	<p>対応する行のログ エントリをエクスポートします。アイコンをクリックすると、詳細な分析やアーカイブの目的でログ エントリをファイルとしてダウンロードできます。</p>

イベント ログのエクスポート

手順

ステップ 1 [Navigation] ペインから、[システム]>[ログ]をクリックします。

ステップ 2 システム イベント ログ タブを選択します。

ステップ 3 すべてのエントリ、単一のエントリ、または特定の数の選択したエントリをエクスポートできます。

a) すべてのログ エントリをエクスポートするには、**すべてエクスポート**。

ブラウザ設定によって、ログ ファイルを開くまたは、保存することをプロンプトされる場合があります。

- b) 1つのエントリをエクスポートするには、対応する行の [エクスポート (export)] アイコンをクリックして、ログ エントリをファイルとしてダウンロードします。

ブラウザ設定によって、ログ ファイルを開くまたは、保存することをプロンプトされる場合があります。

- c) 特定の数のエントリをエクスポートするには、エクスポートするログ行に対応するチェックボックスをオンにします。

チェック ボックスをオンにする時、追加オプションを含む新しいヘッダー行がテーブルの上に現れます。登録手続きを開始するには、**エクスポート**。ブラウザ設定によって、ログ ファイルを開くまたは、保存することをプロンプトされる場合があります。

システム イベント ログの削除

手順

ステップ 1 [Navigation] ペインから、[システム]>[ログ]をクリックします。

ステップ 2 システム イベント ログ タブを選択します。

ステップ 3 すべてのログ エントリを削除するには、**すべて削除する**。

(注)

一度にすべてのエントリを削除することは可能ですが、個々のエントリまたは特定の選択されたエントリを削除することはサポートされていません。

ステップ 4 リスト ログの削除 ダイアログボックスで、**削除 (Delete)** をクリックして確認します。

POST ログ

POST コードログの表示

手順

ステップ 1 [Navigation] ペインから、[システム]>[ログ]をクリックします。

ステップ 2 POST ログ タブを選択します。

ステップ 3 次のオプションに基づいてログをフィルタ処理できます。

- 開始と終了の日付
- 検索フィールドを使用して検索キーワード

ステップ4 次のログ プロパティを表示することができます：

名前	説明
Created column	POST コードログが生成された日時を表示します。
タイムスタンプオフセット column	POST コードがログに記録されたときのシステム開始からの時間オフセットを示します。
ブート回数 column	システムが起動した回数を表示します。
POSTコード column	電源投入時セルフテスト (POST) コードを表示します。

POST コード ログのエクスポート

手順

ステップ1 [Navigation] ペインから、[システム]>[ログ]をクリックします。

ステップ2 POST ログ タブを選択します。

ステップ3 すべてのログ エントリをエクスポートするには、[すべてエクスポート (Export all)] をクリックします。
すべてエクスポート。

ブラウザ設定によって、ログファイルを開くまたは、保存することをプロンプトされる場合があります。

テクニカル サポート ログ

テクニカル サポート ログのエクスポート

手順

ステップ1 [Navigation] ペインから、[管理]>[ユーティリティ]をクリックします。

ステップ2 通常の テクニカルサポートログのエクスポートの場合、 ログのエクスポート。

[レガシー モード構成 (Legacy mode configuration)] ダイアログボックスが表示されます。

ステップ 3 次に [レガシー モード構成 (Legacy mode configuration)] ダイアログ ボックスで、次のように更新します。

名前	説明
[外部サーバ URI (External Server URI)] field	<p>ログをエクスポートする外部サーバの URI を入力します。次のいずれかの形式を使用できます。</p> <ul style="list-style-type: none"> • IPv4 または IPv6 形式の IP アドレス。 • 完全修飾ドメイン名 (FQDN) (Fully Qualified Domain Name (FQDN))
画像へのパス field	<p>外部サーバでログを保存するパスを入力します。英数字と特殊文字+。</p> <ul style="list-style-type: none"> • \ (バックスラッシュ) • / (スラッシュ) • _ (アンダースコア) • - (ハイフン) • . (ドット) <p>このフィールドに入力できる最大文字数は 256 文字です。</p>
マウントタイプ オプション ボタン	<p>外部サーバにログを転送するプロトコルを選択します。次のオプションのいずれかを選択します。</p> <ul style="list-style-type: none"> • TFTP トリビアル ファイル転送プロトコル • SFTP セキュア ファイル転送プロトコル • FTP : ファイル転送プロトコル • SCP セキュア コピー プロトコル • HTTP ハイパーテキスト転送プロトコル

ステップ 4 [保存 (Save)] を [Save]。

テクニカル サポート ログのダウンロード

手順

ステップ 1 **[Navigation]** ペインから、**[管理]** > **[ユーティリティ]** をクリックします。

ステップ 2 通常の テクニカルサポートログのエクスポートの場合、**ログのダウンロード**。

ログファイルが存在しない場合は、次のメッセージが表示されることがあります。

収集されたテクニカル サポート ログ ファイルがありません。新しくログの収集を開始しますか？

登録手続きを開始するには、**確認 (Confirm)** を選択して続行します。



第 10 章

ユーティリティとイベント管理の構成

- イベント管理設定の構成 (103 ページ)
- 実践中 Cisco BMC 2.0 工場出荷時の状態へのリセット (104 ページ)
- リポート Cisco BMC 2.0 (104 ページ)

イベント管理設定の構成

手順

ステップ 1 [Navigation] ペインから、[管理]>[イベント管理]をクリックします。

ステップ 2 次のプロパティを更新できます。

名前	説明
すべてのイベントフィルタの有効化/無効化 トグル ボタン	すべてのイベントフィルタを一度に有効または無効にします。この基準を活用、すべてのイベントのアラートを制御します。
範囲外の温度センサー トグル ボタン	許容範囲外の値を報告する温度センサーのアラートを有効または無効にします。
プロセッサのプレゼンス トグル ボタン	プロセッサの存在またはステータスに関連するイベントのアラートを有効または無効にします。
範囲外の電圧センサー トグル ボタン	許容範囲外の値を報告する電圧センサーのアラートを有効または無効にします。
ウォッチドッグ タイマー トグル ボタン	ウォッチドッグ タイマーによってトリガされるアラートを有効または無効にします。ウォッチドッグ タイマーは、システムをモニタし、無応答状態の間にリセットします。

ステップ3 登録手続きを開始するには、設定の保存。

実践中 Cisco BMC 2.0 工場出荷時の状態へのリセット

値は、Cisco BMC 2.0 は、再起動プロセス中一時的に使用できません。

始める前に

初期設定へのリセットを実行する前に、必要なすべての構成および設定が外部に文書化されているか、または外部に保存されていることを確認してください。このプロセスにより、デバイスはデフォルト設定に復元され、既存の構成がすべて削除されます。

手順

ステップ1 [Navigation] ペインから、[管理]>[ユーティリティ]をクリックします。

ステップ2 通常の工場出荷時の状態へのリセットの場合、復元上に構築できます。

この Cisco BMC 2.0 は再起動し、デフォルト設定は再起動後に適用されます。

リブート Cisco BMC 2.0

手順

ステップ1 [Navigation] ペインから、[管理]>[ユーティリティ]をクリックします。

ステップ2 通常のリブート BMC の場合、リブート BMC 上に構築できます。

この Cisco BMC 2.0 は、再起動プロセス中一時的に使用できません。



第 11 章

ファームウェアの管理

- [ファームウェア管理の概要 \(105 ページ\)](#)
- [ファームウェア コンポーネントの表示 \(105 ページ\)](#)
- [BMC ファームウェアのアップデート \(106 ページ\)](#)

ファームウェア管理の概要

次のファームウェア コンポーネントを表示できます。

- BMC
- BIOS
- FPGA

以下から BMC ファームウェア コンポーネントを更新できます Cisco BMC 2.0。

ファームウェア コンポーネントの表示

手順

ステップ 1 [Navigation] ペインから、[管理]>[ファームウェア管理]をクリックします。

ステップ 2 通常の BMC では、次を表示できます。

名前	説明
Version column	BMC 上で実行中のイメージの現在のバージョンを表示します。

ステップ 3 通常の BIOS では、次を表示できます。

名前	説明
Version column	BIOS 上で実行中のイメージの現在のバージョンが表示されます。

ステップ 4 通常の **FPGA** では、次を表示できます。

名前	説明
[名前 (Name)] column	FPGA コンポーネントの名前を表示します。
Version column	BIOS 上で実行中のイメージの現在のバージョンが表示されます。

BMC ファームウェアのアップデート

手順

-
- ステップ 1 [Navigation] ペインから、[管理]>[ファームウェア管理]をクリックします。
 - ステップ 2 通常の **BMC**ファームウェアの更新の場合、ファイルの追加。
 - ステップ 3 ローカル マシンから適切なイメージファイルを選択します。
 - ステップ 4 登録手続きを開始するには、更新の開始 ファームウェアの更新を開始します。
-



第 12 章

コミュニケーションサービスの設定

- TLS の有効化または無効化 (107 ページ)
- IPMI の設定 (108 ページ)
- SSH の設定 (108 ページ)
- SOL不揮発性ビットレートの構成 (109 ページ)
- Web セッションタイムアウトの構成 (109 ページ)
- OpenSSL FIPS モードの有効化または無効化 (110 ページ)
- Web ポート値の構成 (110 ページ)
- 電子メールアラートを受信するための SMTP サーバの構成 (111 ページ)

TLS の有効化または無効化

始める前に

[InterTenantFW] が **プライマリ設定** または **セカンダリ設定** (または両方) が、それぞれの構成で TLS を有効にする前に有効になっています。

手順

ステップ 1 [Navigation] ペインから、[管理] > [通信サービス] をクリックします。

ステップ 2 メールアラート タブを選択します。

ステップ 3 TLS を有効にする構成 (プライマリまたはセカンダリ) を探します。

ステップ 4 選択した構成の下で、TLS Enable ボタンを有効にして、電子メール通信の保護に Transport Layer Security を使用します。

TLS を有効にすると、次の証明書フィールドが表示されます。

- Cacert PEM証明書
- サーバーCRT証明書
- サーバーキー証明書

ステップ5 各証明書フィールド：

- a) [削除 ファイルの追加] も変更されます。
- b) ローカル マシンから適切な証明書ファイルを選択します。
- c) アップロードを確認して、ファイルをそれぞれのフィールドに関連付けます。

IPMI の設定

サーバプラットフォームに組み込まれているサービス プロセッサとの通信プロトコルを定義します。IPMIは、システムの正常性（温度、ファン速度、電圧など）をモニタし、ハードウェアコンポーネントを制御して潜在的な問題に対処することで、能動的システム管理を可能にします。たとえば、サーバの温度が指定されているレベルより高くなった場合、BMC はファン速度を上げたり、プロセッサの速度を下げたりするなどの是正措置を講じて、システムを冷却し、安定性を維持できます。

IPMI（アウトオブバンド）の構成

手順

-
- ステップ1 [Navigation] ペインから、[管理]>[通信サービス]をクリックします。
 - ステップ2 通信サービス タブを選択します。
 - ステップ3 通常の サービスLocate ネットワークIPMI (アウトオブバンドIPMI)。
 - ステップ4 この機能を有効または無効にするには、トグル ボタンを使用します。
-

SSH の設定

始める前に

手順

-
- ステップ1 a)
 - ステップ2
 - ステップ3
-

次のタスク

SOL不揮発性ビットレートの構成

手順

ステップ1 [Navigation] ペインから、[管理]>[通信サービス]をクリックします。

ステップ2 通信サービス タブを選択します。

ステップ3 通常の SOL SSHの下で、次のプロパティを更新します。

名前	説明
SOL SSHの有効化 トグル ボタン	以下の SOL SSH オプションを切り替えて、Serial over LAN (SOL) のセキュア シェル (SSH) サービスを有効にします。SOL の管理にSSHアクセスが必要な場合は、このオプションを使用します。
SOL SSHポート値(数値)	(注) このオプションは、SOL SSHが有効になっている場合にのみ表示されます。 フィールドに数値を入力して、SOL SSHのポートを指定します。または、フィールドの末尾にある上矢印または下矢印を使用して、ポート番号を1ずつ増減することもできます。
[Save] ボタン	[保存 (Save)] をクリックして設定を保存します。

Web セッション タイムアウトの構成

Webセッションタイムアウト 値は、Webセッションが自動的に期限切れになるまでの非アクティブ期間を決定します。

手順

ステップ1 [Navigation] ペインから、[管理]>[通信サービス]をクリックします。

ステップ2 通信サービス タブを選択します。

ステップ3 通常の **Webセッションタイムアウト**、このフィールドに30秒から86400までの数値を入力して、セッションタイムアウトを秒単位で指定します。

ステップ4 [保存 (Save)] を [Save]。

OpenSSL FIPS モードの有効化または無効化

OpenSSL FIPSモードを有効にすると、暗号化操作がFIPS 140-2 標準に準拠するようになります。FIPS準拠のセキュリティが必要な環境の場合は、このオプションをします。

手順

ステップ1 [Navigation] ペインから、[管理]>[通信サービス]をクリックします。

ステップ2 通信サービス タブを選択します。

ステップ3 通常の **OpenSSL FIPSモード**以下をトグルし、**OpenSSL FIPS モードの有効化** Federal Information Processing Standards (FIPS) をアクティブ化します。

Web ポート値の構成

Webインターフェイスを使用してシステムを構成する場合は、[Webポート値 (Web Port Value)]によって、Web サーバが HTTP または HTTPS トラフィックを受け入れる特定のポートが決まります。

手順

ステップ1 [Navigation] ペインから、[管理]>[通信サービス]をクリックします。

ステップ2 通信サービス タブを選択します。

ステップ3 通常の **Webポート値(数値)**で、このフィールドに数値を入力して、Web アクセスに使用するポートを指定します。値が、システムで実行中の他のサービスと競合しないことを確認してください。

ステップ4 [保存 (Save)] を [Save]。

電子メールアラートを受信するためのSMTPサーバの構成

始める前に

[InterTenantFW] が **プライマリ設定** または **セカンダリ設定** トグル ボタンが **有効** をクリックします。設定を有効にした後にのみサーバを構成できます。

手順

ステップ 1 [Navigation] ペインから、[管理] > [通信サービス] をクリックします。

ステップ 2 メールアラート タブを選択します。

ステップ 3 [プライマリ設定] または [セカンダリ設定] または両方を有効状態にします。

ステップ 4 各構成の下で次のプロパティを更新します。

名前	説明
認証 トグル ボタン	電子メールサーバで認証が必要な場合に有効にします。これを有効にすると、[ユーザー名 (Username)] と [パスワード (Password)] フィールドが表示されます。認証が不要な場合は、無効のままにします。
[ユーザー名 (Username)] field	認証用のユーザー名を入力します。このフィールドは、認証が有効になっている場合にのみ表示されます。
パスワード (Password) field	認証用のパスワードを入力します。このフィールドは、認証が有効になっている場合にのみ表示されます。
サーバーアドレス (Server Address) field	電子メールサーバのアドレスを入力します。
ポート field	電子メールサーバに接続するために使用するポート番号を入力します。
送信者の電子メールアドレス field	アラートを送信する電子メールアドレスを入力します。
受信者の電子メールアドレスの追加	クリックして、受信者の電子メールアドレスのフィールドを追加します。
受信者の電子メールアドレス field	受信者の電子メールアドレスを入力します。デフォルトで表示されます。

名前	説明
TLS Enable トグル ボタン	電子メール通信のセキュリティを保護するためにTransport Layer Security (TLS) を使用するには、このオプションを有効にします。電子メールサーバがTLSをサポートしている、または必要としている場合に使用します。TLSが不要な場合は、無効のままにします。

ステップ5 登録手続きを開始するには、**設定の保存**。

次のタスク

登録手続きを開始するには、**テストアラートの送信** ボタンをクリックすると、設定を使用してテスト電子メールアラートを送信できます。これを活用、電子メールアラート構成が期待どおりに機能していることを確認します。

電子メール受信者の追加

始める前に

[InterTenantFW] が **プライマリ設定** または **セカンダリ設定** トグル ボタンは、**有効** をクリックします。この **受信者の電子メールアドレスの追加** オプションは、有効になっている設定の下でのみ表示されます。

手順

ステップ1 [Navigation] ペインから、[管理]>[通信サービス]をクリックします。

ステップ2 メールアラート タブを選択します。

ステップ3 通常の **プライマリ設定** または **セカンダリ設定** の場合、**受信者の電子メールアドレスの追加** をクリックして、新しい受信者の電子メールアドレス フィールドを追加します。

(注)

[**受信者の電子メール アドレス 1 (Recipient Email Address 1)**] は、デフォルトでは存在しません。クリックするたびに、受信者の電子メールアドレス フィールドが追加されます。

ステップ4 新しく追加されたフィールドに電子メールアドレスを入力します。

必要な場合は、手順3 と 4 を繰り返して電子メールアドレスを追加します。

ステップ5 [設定の保存 (Save Settings)] をクリックします。



第 13 章

Device Connector の管理

- [Intersight 管理モード](#) (113 ページ)
- [デバイス コネクタを有効化または無効化](#) (114 ページ)
- [プロキシ設定](#) (114 ページ)
- [証明書のインポートまたは、表示](#) (115 ページ)
- [アプライアンス接続のチェック](#) (116 ページ)

Intersight 管理モード

Cisco Intersight は、シスコとサードパーティの IT インフラストラクチャ向けの分析機能が組み込まれた SaaS 方式の管理プラットフォームです。Intersight Managed Mode (IMM) は、Redfish ベースの標準モデルを通じて UCS ファブリックインターコネクトシステムを管理する新しいアーキテクチャです。Intersight マネージドモードは、UCS システムの機能と Intersight のクラウドベースの柔軟性を統合し、スタンドアロンおよびファブリックインターコネクト接続システムの管理エクスペリエンスを統合します。

Cisco ベースボード管理コントローラ 2.0 REST API ガイド、リリース 2.0 デバイス コネクタが Cisco Intersight サービスへの接続を検出しない場合、次の警告を表示します。

デバイス コネクタは、Cisco Intersight に対しての接続を検出できません。設定を確認し、サーバーが Intersight インフラストラクチャ サービス ライセンスに準拠して Intersight で要求されていることを確認してください。(1/5)

以下をクリックします **[OK]** をクリックします [デバイス コネクタ (Device Connector)] に移動し、設定を構成するか、**キャンセル** をクリックして続行します。

警告とは別に、Cisco BMC 2.0 画面の上部に次の静的リボンも表示します：

注：このサーバーには、Intersight インフラストラクチャ サービス ライセンス ライセンスが必要です。詳しくはこちら

詳細をクリックすると、Intersight ヘルプ センターから詳細情報を取得できます。



(注) このメッセージは、デバイス コネクタが構成されている場合は表示されません。デバイス コネクタを一度構成し、後で無効にすると、メッセージが再度表示されます。

デバイス コネクタを有効化または無効化

手順

ステップ1 [Navigation] ペインから、[管理]>[デバイス コネクタ]をクリックします。

ステップ2 [設定] アイコンをクリックします。

[設定] ナビゲーションが表示されます。

ステップ3 選択 **全般** をクリックします。

次のプロパティを表示または、アップデートすることができます：

名前	説明
デバイス コネクタ トグル ボタン	<p>Intersight の管理を有効または無効にできます。次のいずれかになります。</p> <ul style="list-style-type: none"> • 点灯：Intersight の管理を有効にします。このシステムに対し要求を行って、Cisco Intersight の機能を活用できます。 • 消灯：Intersight 管理を無効にします。Cisco Intersight への通信は許可されません。

ステップ4 [保存 (Save)] をクリックします。

プロキシ設定

手順

ステップ1 [Navigation] ペインから、[管理]>[デバイス コネクタ]をクリックします。

ステップ2 [設定] アイコンをクリックします。

[設定] ナビゲーションが表示されます。

ステップ 3 選択 プロキシ設定。

次のプロパティを表示または、アップデートすることができます：

名前	説明
プロキシを有効にする トグル ボタン	HTTPS プロキシ設定を有効または無効にすることができます。
プロキシホスト名/IP field	プロキシ サーバーの IP アドレスまたはホスト名。
プロキシポート field	プロキシ サーバーのポート番号。
認証 トグル ボタン	このオプションを有効にすると、プロキシサーバーのクレデンシャルを提供できます。
[ユーザー名 (Username)] field	プロキシ サーバーのクレデンシャルです。
パスワード (Password) field	

ステップ 4 [保存 (Save)] を [Save]。

証明書のインポートまたは、表示

手順

ステップ 1 [Navigation] ペインから、[管理] > [デバイス コネクタ] をクリックします。

ステップ 2 [設定] アイコンをクリックします。

[設定] ナビゲーションが表示されます。

ステップ 3 選択 証明書マネージャ。

次のプロパティを表示または、アップデートすることができます：

表 35: 証明書マネージャ

名前	説明
インポート (Import) ボタン	CA 署名付き証明書を選択してインポートすることができます。 (注) インポートされた証明書が *.pem (base64 エンコード) 形式である必要があります。

名前	説明
[名前 (Name)] column	CA 証明書の共通名。
使用中 column	トラストストアでリモートサーバーを正しく確認するため証明書を使用したかどうか。
発行元 (Issued By) column	証明書の発行機関。
Expires column	証明書の有効期限日。
[View Certificate] アイコン	クリックして証明書の詳細を表示します。
証明書の削除 ボタン	証明書を削除できます。 (注) バンドルされている証明書(ロックアイコンが証明書)を削除することはできません。

アプライアンス接続のチェック

手順

ステップ 1 [Navigation] ペインから、[管理]>[デバイス コネクタ]をクリックします。

ステップ 2 [設定] アイコンをクリックします。

[設定] ナビゲーションが表示されます。

ステップ 3 選択 **接続** をクリックします。

ステップ 4 From the **接続の確認** ドロップダウン リストから、接続を確認するアプライアンスを選択します。

次のプロパティを表示することができます：

表 36: 接続

名前	説明
詳細を表示	以下を表示できます。 アドレス および 遅延 (Latency) DNS 解決の値を入力します。
デバッグ ログ	デバッグ ログを表示できます。

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。