Cisco UCS C シリーズ Integrated Management Controller リリース 3.1 GUI コンフィギュレーション ガイド

初版：2017 年 08 月 17 日

最終更新：2017 年 10 月 10 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/

【注意】シスコ製品をご使用になる前に、安全上の注意（**www.cisco.com/jp/go/safety_warning/**）をご確認ください。本書は、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。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

目 次

はじめに

この前書きは、次のセクションで構成されています。

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	表示
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、[GUI 要素] のように示しています。 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、[メインタイトル] のように示しています。
マニュアルのタイトル	マニュアルのタイトルは、イタリック体（*Italic*）で示しています。

テキストのタイプ	表示
TUI 要素	テキストベースのユーザ 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、courier フォントで示しています。
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、courier フォントで示しています。
CLI コマンド	CLI コマンドのキーワードは、ボールド体 **this font** で示しています。 CLI コマンド内の変数は、イタリック体 *this font* で示しています。
[ ]	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）「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「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「時間の節約に役立つ操作」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 「要注意」の意味です。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 IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger.You are in a situation that could cause bodily injury.Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device.

SAVE THESE INSTRUCTIONS

関連する Cisco UCS ドキュメント

ドキュメント ロードマップ

すべての B シリーズ マニュアルの完全なリストについては、『*Cisco UCS B-Series Servers Documentation Roadmap*』（URL：http://www.cisco.com/go/unifiedcomputing/b-series-doc）を参照してください。

すべての C シリーズ マニュアルの一覧については、http://www.cisco.com/go/unifiedcomputing/c-series-doc で入手できる『*Cisco UCS C-Series Servers Documentation Roadmap*』を参照してください。

管理用の UCS Manager と統合されたラック サーバでサポートされるファームウェア バージョンとサポートされる UCS Manager バージョンについては、『Release Bundle Contents for Cisco UCS Software』を参照してください。

その他のマニュアル リソース

ドキュメントの更新通知を受け取るには、Twitter の Cisco UCS Docs をフォローしてください。

第 1 章

概要

この章の内容は、次のとおりです。

Cisco UCS C シリーズ ラックマウント サーバの概要

Cisco UCS C シリーズ ラックマウント サーバには、次のモデルがあります。

- Cisco UCS C220 M5 ラックマウント サーバ
- Cisco UCS C240 M5 ラックマウント サーバ

（注） どの Cisco UCS C シリーズ ラックマウント サーバがこのファームウェア リリースでサポートされているかを判断するには、関連するリリース ノートを参照してください。C シリーズのリリース ノートは次の URL で入手できます。http://www.cisco.com/en/US/products/ps10739/prod_release_notes_list.html

サーバ ソフトウェアの概要

Cisco UCS C シリーズ ラックマウント サーバには Cisco IMC ファームウェアが付属しています。

Cisco IMC ファームウェア

Cisco IMC 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、Cisco IMC ファームウェアを実行します。システムには Cisco IMC ファームウェアの実行バージョンが付属しています。Cisco IMC ファームウェアは更新できますが、初期インストールは必要ではありません。

サーバ OS

Cisco UCS C シリーズ ラック サーバは、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。サポートされているオペレーティング システムの詳細については、『*Hardware and Software Interoperability for Standalone C-series servers*』（http://www.cisco.com/en/US/products/ps10477/prod_technical_reference_list.html）を参照してください。KVM コンソールおよび vMedia を使用してサーバに OS をインストールするために、Cisco IMC を使用できます。

（注） 使用可能な OS のインストール マニュアルには、http://www.cisco.com/go/unifiedcomputing/c-series-doc で『*Cisco UCS C-Series Servers Documentation Roadmap*』からアクセスできます。

Cisco Integrated Management Controller

Cisco IMC は、C シリーズ サーバ用の管理サービスです。Cisco IMC はサーバ内で動作します。

（注） Cisco IMC 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。C シリーズ サーバが UCS システムに統合されている場合は、UCS Manager を使用してそのサーバを管理する必要があります。UCS Manager の使用方法については、http://www.cisco.com/go/unifiedcomputing/b-series-doc の『*Cisco UCS B-Series Servers Documentation Roadmap*』にリストされた設定ガイドを参照してください。

管理インターフェイス

Web ベースの GUI または SSH ベースの CLI または XML ベースの API を使用して、サーバにアクセスし、サーバを設定、管理、モニタできます。ほとんどすべてのタスクは、これらのインターフェイスのいずれでも実行できます。また、一方のインターフェイスで実行されたタスクの結果は、もう一方のインターフェイスにも表示されます。ただし、次の操作はできません。

- Cisco IMC CLI を呼び出すために Cisco IMC GUI を使用する
- Cisco IMC CLI で呼び出したコマンドを Cisco IMC GUI に表示する
- Cisco IMC GUI から Cisco IMC CLI 出力を生成する

Cisco IMC で実行可能なタスク

Cisco IMC を使用すると次のシャーシ管理タスクを実行できます。

- サーバの電源のオン、電源のオフ、電源再投入、リセット、およびシャットダウンを行う
- ロケータ LED を切り替える
- サーバのブート順を設定する
- サーバのプロパティとセンサーを表示する
- リモート プレゼンスの管理
- ローカル ユーザ アカウントを作成して管理し、Active Directory によるリモート ユーザの認証をイネーブルにする
- NIC プロパティ、IPv4、VLAN、ネットワーク セキュリティなど、ネットワーク関連の設定を行う
- HTTP、SSH、IPMI Over LAN、SNMP などのコミュニケーション サービスを設定する
- 証明書を管理する
- プラットフォーム イベント フィルタの設定
- Cisco IMC ファームウェアを更新する
- 障害、アラーム、およびサーバのステータスのモニタ
- タイム ゾーンを設定し、ローカル タイムを表示する
- Cisco IMC ファームウェアをインストールしてアクティブにする
- BIOS ファームウェアをインストールしてアクティブにする
- CMC ファームウェアをインストールしてアクティブにする

Cisco IMC を使用すると次のサーバ管理タスクを実行できます。

- リモート プレゼンスの管理
- ローカル ユーザ アカウントを作成して管理し、Active Directory によるリモート ユーザの認証をイネーブルにする
- NIC プロパティ、IPv4、VLAN、ネットワーク セキュリティなど、ネットワーク関連の設定を行う
- HTTP、SSH、IPMI Over LAN、SNMP などのコミュニケーション サービスを設定する
- 証明書を管理する
- プラットフォーム イベント フィルタの設定
- Cisco IMC ファームウェアを更新する
- 障害、アラーム、およびサーバのステータスのモニタ
- タイム ゾーンを設定し、ローカル タイムを表示する

オペレーティング システムやアプリケーションのプロビジョニングや管理はできない

Cisco IMC はサーバのプロビジョニングを行うため、サーバのオペレーティング システムの下に存在します。したがって、サーバでオペレーティング システムやアプリケーションのプロビジョニングや管理を行うためにこれを使用することはできません。たとえば、次の操作を実行することはできません。

- Windows や Linux などの OS の展開
- OS やアプリケーションなどのソフトウェアに対するパッチの展開
- アンチウイルス ソフトウェア、モニタリング エージェント、バックアップ クライアントなどのベース ソフトウェア コンポーネントのインストール
- データベース、アプリケーション サーバ ソフトウェア、Web サーバなどのソフトウェア アプリケーションのインストール
- Oracle データベースの再起動、プリンタ キューの再起動、または Cisco IMC 以外のユーザ アカウントの処理を含むオペレータ処理の実行
- SAN や NAS ストレージ上の外部ストレージの設定または管理

Cisco IMC ユーザ インターフェイスの概要

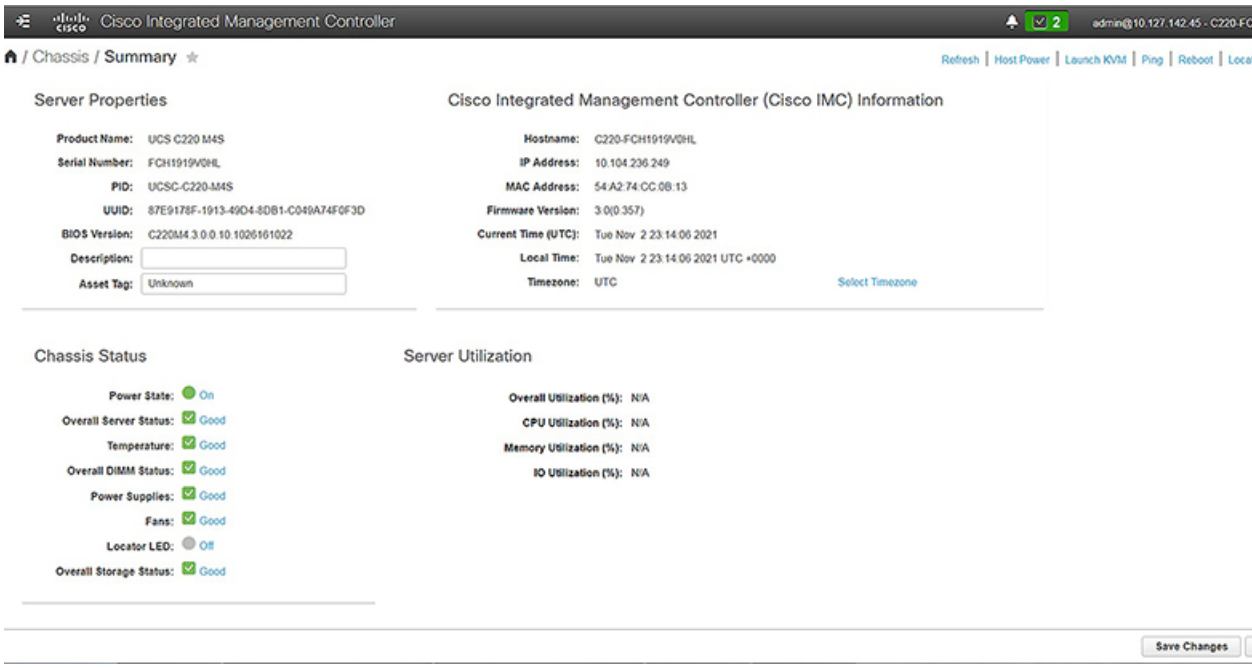
Cisco IMC ユーザ インターフェイスは、Cisco C シリーズ サーバの Web ベースの管理インターフェイスです。Web ユーザ インターフェイスは、eXtensible Widget Framework（XWT）フレームワークを使った HTML5 を使用して開発されます。ユーザ インターフェイスを起動して、次の最小要件を満たしている任意のリモート ホストからサーバを管理できます。

- Microsoft Internet Explorer 6.0 以降、Mozilla Firefox 3.0 以降
- Microsoft Windows 7、Microsoft Windows XP、Microsoft Windows Vista、Apple Mac OS X v10.6、Red Hat Enterprise Linux 5.0 以降のオペレーティング システム
- Transport Layer Security（TLS）バージョン 1.2

（注） Cisco IMC へのログインに使用するパスワードを失効した場合やパスワードを忘れた場合は、使用しているサーバの Cisco UCS C シリーズ サーバのインストレーションおよびサービス ガイドでパスワードの回復手順を参照してください。このガイドは http://www.cisco.com/go/unifiedcomputing/c-series-doc で『*Cisco UCS C-Series Servers Documentation Roadmap*』から入手できます。

Cisco IMC ホームページ

Cisco IMC GUI に初めてログインすると、次の図のようなユーザ インターフェイスが表示されます。



[ナビゲーション（Navigation）] ペインと [作業（Work）] ペイン

Cisco Integrated Management Controller GUI は、画面の左側にある [ナビゲーション（Navigation）] ペインと、画面の右側にある [作業（Work）] ペインで構成されます。[ナビゲーション（Navigation）] ペインの [シャーシ（Chassis）]、[コンピューティング（Compute）]、[ネットワーク（Networking）]、[ストレージ（Storage）]、または [管理者（Admin）] メニューにあるリンクをクリックすると、右側のペインに関連付けられたタブが表示されます。

[ナビゲーション（Navigation）] ペインのヘッダーにはアクション ボタンが表示され、GUI 全体のナビゲーション マップを表示したり、インデックスを表示したり、お気に入りの作業ペインを選択して直接移動したりできます。[Pin] アイコンは、[作業（Work）] ペインが表示されたときに [ナビゲーション（Navigation）] ペインがスライドしないようにします。

[お気に入り（Favorite）] アイコンは星形のボタンで、アプリケーション内の特定の作業ペインをお気に入りに設定できます。これを行うには、選択した作業ウィンドウに移動して、[お気に入り（Favorite）] アイコンをクリックします。アプリケーションの任意の場所からこの作業ウィンドウに直接アクセスするには、[お気に入り（Favorite）] アイコンを再度クリックします。

GUI ヘッダーには、シャーシの全体的なステータスに関する情報およびユーザ ログイン情報が表示されます。

GUI ヘッダーには、障害の総数（緑色または赤色で示されます）も表示され、その横に [ベル（Bell）] アイコンが付いています。ただし、このアイコンをクリックすると、さまざまなコンポーネントの致命的または重大な障害の概要のみが表示されます。すべての障害を表示するには、[すべて表示（View All）] ボタンをクリックして [障害サマリー（Fault Summary）] ペインを表示させます。

（注） ユーザ インターフェイスのオプションは、サーバによって異なります。

[ナビゲーション（Navigation）] ペインには次のメニューがあります。

- [シャーシ（Chassis）] メニュー
- [コンピューティング（Compute）] メニュー
- [ネットワーク（Networking）] メニュー
- [ストレージ（Storage）] メニュー
- [管理者（Admin）] メニュー

[シャーシ（Chassis）] メニュー

[シャーシ（Chassis）] メニューの各ノードは、[作業（Work）] ペインに表示される 1 つ以上のタブに続きます。これらのタブからは次の情報へアクセスできます。

[シャーシ（Chassis）] メニューのノード名	[作業（Work）] ペインのタブで提供される情報
要約	サーバ プロパティ、シャーシ ステータス、Cisco IMC 情報、およびサーバ使用率。
インベントリ	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 エクスパンダ、および TPM。
[センサー（Sensors）]	電源装置、ファン、温度、電圧、電流、LED の読み取り装置、およびストレージ。
電源管理	電力制限の設定と電源監視。 （注） このオプションを使用できるのは一部の UCS C シリーズ サーバだけです。
[障害およびログ（Faults and Logs）]	障害サマリー、障害履歴、システム イベント ログ、Cisco IMC ログおよびロギング制御。

[コンピューティング（Compute）] メニュー

[コンピューティング（Compute）] メニューにはサーバに関する情報が含まれており、次の情報が [作業（Work）] ペインに表示されます。

[コンピューティング（Compute）] メニューのノード名	[作業（Work）] ペインのタブで提供される情報
[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。
BIOS	インストール済みの BIOS ファームウェア バージョン、およびサーバのブート順。
[トラブルシューティング（Troubleshooting）]	ブートストラップ処理、クラッシュ レコーディング、最後に保存したブートストラップ プロセスを表示するプレーヤー。
[電源ポリシー（Power Policies）]	電源復元ポリシーの設定。
PID カタログ	CPU、メモリ、PCI アダプタ、および HDD の詳細。

[ネットワーク（Networking）] メニュー

[ネットワーク（Networking）] メニューの各ノードは、[作業（Work）] ペインに表示される 1 つ以上のタブに続きます。これらのタブからは次の情報へアクセスできます。

[ネットワーク（Networking）] メニューのノード名	[作業（Work）] ペインのタブで提供される情報
一般	アダプタ カードのプロパティ、ファームウェア、外部イーサネットインターフェイス、設定をエクスポートまたはインポートするアクション、リセット ステータス。
[vNIC]	名前、CDN、MAC アドレス、MTU、個々の vNIC プロパティなどのホスト イーサネット インターフェイス情報。
[vHBA]	名前、WWPN、WWNN、ブート、アップリンク、ポートプロファイル、チャネル番号、個々の vHBA プロパティなどのホスト ファイバ チャネル インターフェイス情報。

[ストレージ（Storage）] メニュー

[ストレージ（Storage）] メニューの各ノードは、Cisco UCS C シリーズ ラックマウント サーバにインストールされた LSI MegaRAID コントローラまたはホスト バス アダプタ（HBA）に対応します。各ノードは、[作業（Work）] ペインに表示される 1 つ以上のタブに続き、インストールされているコントローラに関する情報を提供します。

[ストレージ（Storage）] メニューのノード名	[作業（Work）] ペインのタブで提供される情報
[コントローラ情報（Controller Info）]	選択した LSI MegaRAID コントローラまたは HBA に関する一般情報。
[物理ドライブ情報（Physical Drive Info）]	一般的なドライブ情報、識別情報、およびドライブのステータス。
仮想ドライブ情報（Virtual Drive Info）	一般的なドライブ情報、RAID 情報、物理ドライブ情報。
バッテリ バックアップ ユニット（Battery Backup Unit）	選択された MegaRAID コントローラのバックアップ バッテリ情報。
ストレージ ログ（Storage Log）	ストレージ メッセージ。

[管理者（Admin）] メニュー

[管理者（Admin）] メニューの各ノードは、[作業（Work）] ペインに表示される 1 つ以上のタブに続きます。これらのタブからは次の情報へアクセスできます。

[管理者（Admin）] メニューのノード名	[作業（Work）] ペインのタブで提供される情報
ユーザ管理	ローカルで定義されたユーザ アカウント、Active Directory 設定、および現在のユーザ セッション情報。
Networking	NIC、IPv4、IPv6、VLAN、LOM プロパティとネットワーク セキュリティ設定。
[コミュニケーション サービス（Communication Services）]	HTTP、SSH、XML API、IPMI over LAN、および SNMP 設定。
証明書の管理（Certificate Management）	セキュリティ証明書情報と管理。
[ファームウェア管理（Firmware Management）]	Cisco IMC および BIOS ファームウェア情報と管理。
[ユーティリティ（Utilities）]	テクニカルサポートデータ収集、システム設定のインポートおよびエクスポートオプション、出荷時の初期状態の復元設定。

[管理者（Admin）] メニューのノード名	[作業（Work）] ペインのタブで提供される情報
デバイス コネクタ	Starship の管理とネットワーク設定。 （注） このオプションを使用できるのは一部の C シリーズ サーバだけです。

ツールバー

ツールバーは [作業（Work）] ペインの上に表示されます。

ボタン名	説明
更新（Refresh）	現在のページを更新します。
[ホストの電源（Host Power）]	表示されるドロップダウン メニューから電源オプションを選択します。
[KVM の起動（Launch KVM）]	Java ベースまたは HTML ベースの KVM コンソールを起動するためのドロップダウン メニューが表示されます。
[ping]	[Ping の詳細（Ping Details）] ポップアップ ウィンドウを起動します。
Reboot	Cisco IMC をリブートできます。
[ロケータ LED（Locator LED）]	ロケータ LED をオンまたはオフにできます。

Cisco Integrated Management Controller オンライン ヘルプの概要

Cisco Integrated Management Controller（Cisco IMC）ソフトウェアの GUI は、左側にある [ナビゲーション（Navigation）] ペインと右側にある [ワーク（Work）] ペインの 2 つの主要なセクションに分かれます。

このヘルプ システムは、各 Cisco IMC Cisco IMC GUI ページと各ダイアログボックスのフィールドについて説明します。

ページのヘルプにアクセスするには、次のいずれかを実行します。

- Cisco IMC Cisco IMC GUI の特定のタブで、[ワーク（Work）] ペインの上のツールバーにある [ヘルプ（Help）] アイコンをクリックします。
- ダイアログボックスで、そのダイアログボックスの [ヘルプ（Help）] ボタンをクリックします。

（注） すべての C シリーズ マニュアルの一覧については、http://www.cisco.com/go/unifiedcomputing/c-series-doc で入手できる『*Cisco UCS C-Series Servers Documentation Roadmap*』を参照してください。

Cisco IMC へのログイン

手順

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

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。

a) （任意） チェックボックスをオンにして、シスコからのすべてのコンテンツを受け入れます。

b) [はい（Yes）] 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。

ヒント 未設定のシステムに対する初回ログイン時には、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。

- Cisco IMC Web UI 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単語「password」を選択することはできません。実行するスクリプトでこの制限が問題になる場合は、ユーザ管理オプションに再びログインしてパスワードを password に変更できますが、これに伴うリスクは完全に自分の責任となります。シスコでは推奨していません。

ステップ 4 [ログイン（Log In）] をクリックします。

Cisco IMC からのログアウト

手順

ステップ 1 Cisco IMC の右上で、[ログアウト（Log Out）] をクリックします。

ログアウトすると、Cisco IMC のログイン ページに戻ります。

ステップ 2 （任意） 再度ログインするか、Web ブラウザを閉じます。

第 2 章

サーバ OS のインストール

この章の内容は、次のとおりです。

OS のインストール方法

C シリーズ サーバは、複数のオペレーティング システムをサポートしています。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
- PXE インストール サーバ

KVM コンソール

KVM コンソールは Cisco IMC からアクセス可能なインターフェイスであり、サーバへのキーボード、ビデオ、マウス（KVM）の直接接続をエミュレートします。KVM 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。

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、KVM 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

KVM 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。

（注） Windows Server 2003 の Internet Explorer 6 SP1 から KVM コンソールを起動すると、必要なファイルをダウンロードできないことがブラウザから報告されます。この場合、ブラウザの [Tools] メニューをクリックし、[Internet Options] を選択します。[Advanced] タブをクリックし、[Security] セクションの [Do not save encrypted pages to disk] チェックボックスをオフにします。KVM コンソールを再度起動します。

KVM コンソールを使用した OS のインストール

（注） この手順では、基本的なインストール手順についてのみ説明します。Linux、VMware、および Windows のインストールの詳細なガイドについては、次の URL を参照してください。http://www.cisco.com/en/US/products/ps10493/products_installation_and_configuration_guides_list.html

はじめる前に

- OS インストール ディスクまたはディスク 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 Cisco IMC が開いていない場合は、ログインします。

ステップ 3 [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 4 [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 5 作業ウィンドウの [リモート管理（Remote Management）] タブをクリックします。

ステップ 6 [リモート管理（Remote Management）] ペインで、[仮想 KVM（Virtual KVM）] タブをクリックします。

ステップ 7 [アクション（Actions）] 領域で、[KVM コンソール起動（Launch KVM Console）] をクリックします。

[KVM コンソール（KVM Console）] が別ウィンドウで開きます。

ステップ 8 KVM コンソールから、[VM] タブをクリックします。

ステップ 9 [VM] タブで、次のいずれかの方法を使用して仮想メディアをマップします。

- OS インストール ディスクが含まれている CD/DVD ドライブの [マップ済み（Mapped）] チェックボックスをオンにします。
- [イメージの追加（Add Image）] をクリックし、OS インストール ディスク イメージに移動してこれを選択します。[開く（Open）] をクリックしてディスク イメージをマウントし、マウントされたディスク イメージの [マップ済み（Mapped）] チェックボックスをオンにします。

（注） OS のインストール プロセスの間は、[VM] タブを開いたままにしておく必要があります。このタブを閉じると、すべての仮想メディアのマップが解除されます。

ステップ 10 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 のインストレーション ガイドを参照してください。

次の作業

OS のインストールが完了したら、仮想メディアのブート順を元の設定にリセットします。

PXE インストール サーバ

Preboot Execution Environment（PXE）インストール サーバを使用すると、クライアントはリモートの場所から OS をブートおよびインストールできます。この方法を使用するには、PXE 環境が設定されていて、VLAN（通常は専用のプロビジョニング VLAN）で使用できるようになっている必要があります。さらに、サーバがネットワークからブートするように設定されている必要があります。サーバは、ブートすると、PXE 要求をネットワーク経由で送信します。PXE インストール サーバは、この要求に応答確認し、サーバに OS をインストールするイベントのシーケンスを開始します。

PXE サーバは、インストール ディスク、ディスク イメージ、またはスクリプトを使用して、OS をインストールできます。また、独自のディスク イメージを使用して、OS、追加コンポーネント、またはアプリケーションをインストールすることもできます。

（注） PXE インストールは、多数のサーバに OS をインストールする場合に効率のよい方法です。ただし、この方法を使用するには PXE 環境をセットアップする必要があることを考えると、他のインストール方法を使用する方が簡単な場合があります。

PXE インストール サーバを使用した OS のインストール

はじめる前に

- VLAN 経由でサーバに到達できることを確認します。
- 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 PXE のブート順を最初に設定します。

ステップ 2 サーバをリブートします。
VLAN で PXE インストール サーバを使用できる場合は、サーバが再起動するとインストール プロセスが開始します。通常、PXE インストールは自動化されており、追加のユーザ入力を必要としません。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 のインストレーション ガイドを参照してください。

次の作業

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。

USB ポートからのオペレーティング システムの起動

すべての Cisco UCS C シリーズ サーバでは、サーバ上の任意の USB ポートからオペレーティング システムを起動できます。ただし、USB ポートから OS を起動する前に、いくつかのガイドラインを考慮する必要があります。

- ブート順序の設定を保持するために、内部 USB ポートを使って OS を起動することをお勧めします。
- USB ポートから OS を起動する前に、そのポートを有効にしておく必要があります。

  デフォルトでは、USB ポートは有効になっています。USB ポートを無効化している場合、そこから OS を起動する前に有効にする必要があります。無効化された USB ポートを有効にする方法については、サーバ固有のインストールおよびサービス ガイドにある『*Enabling or Disabling the Internal USB Port*』のトピックを参照してください。次のリンクを利用できます。

  http://www.cisco.com/en/US/products/ps10493/prod_installation_guides_list.html.
- USB ポートから OS を起動した後、その USB ソースからサーバが毎回ブートするよう、下位レベルのブート順序を設定する必要があります。

第 3 章

シャーシの管理

この章の内容は、次のとおりです。

シャーシ要約（Chassis Summary）

シャーシ要約の表示

デフォルトでは、Cisco UCS C シリーズ ラックマウント サーバにログオンすると、シャーシの [サマリー（Summary）] ペインが Web UI に表示されます。次の手順を実行することで、別のタブまたは作業領域を開いている際に、シャーシのサマリーを表示することもできます。

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 [サマリー（Summary）] をクリックします。

ステップ 3 [シャーシ要約（Chassis Summary）] ペインの [サーバ プロパティ（Server Properties）] 領域で、次の情報を確認します。

[名前（Name）]	説明
[製品名（Product Name）] フィールド	サーバのモデル名。
[シリアル番号（Serial Number）] フィールド	サーバのシリアル番号。
[PID] フィールド	製品 ID。

[名前（Name）]	説明
[UUID] フィールド	サーバに割り当てられている UUID。
[BIOS バージョン（BIOS version）] フィールド	サーバで実行されている BIOS のバージョン。
[説明（Description）] フィールド	サーバのユーザ定義の説明。
[アセット タグ（Asset Tag）] フィールド	サーバのユーザ定義のタグ。デフォルトでは、新しいサーバのアセット タグには [不明（Unknown）] と表示されます。

ステップ 4 [シャーシ要約（Chassis Summary）] ペインの [Cisco IMC 情報（Cisco IMC Information）] 領域で、次の情報を確認します。

[名前（Name）]	説明
[ホスト名（Hostname）] フィールド	Cisco IMC のユーザ定義のホスト名。デフォルトでは、ホスト名はCXXX-YYYYYY 形式で表示されます（XXX はサーバのモデル番号、YYYYYY はシリアル番号です）。
[IPアドレス（IP Address）] フィールド	Cisco IMC の IP アドレス
[MACアドレス（MAC Address）] フィールド	Cisco IMC に対するアクティブなネットワーク インターフェイスに割り当てられている MAC アドレス。
[ファームウェアバージョン（Firmware Version）] フィールド	現在の Cisco IMC ファームウェアのバージョン。
[現在の時刻（Current Time）] フィールド	Cisco IMC クロックが示している現在の日時。 （注） NTP が無効になっている場合、Cisco IMC は、サーバ BIOS から現在の日時を取得します。NTP を有効にすると、Cisco IMC は現在の時刻と日付を NTP サーバから取得します。この情報を変更するには、サーバをリブートし、BIOS 設定メニューへのアクセスに関するメッセージが表示されたら F2 キーを押します。メインの BIOS 設定タブでオプションを使用して日付または時刻を変更します。
[ローカル タイム（Local Time）] フィールド	選択したタイム ゾーンに準じた地域のローカル タイム。

[名前（Name）]	説明
[タイムゾーン（Timezone）] フィールド	[タイムゾーンの選択（Select Timezone）] オプションをクリックして、タイム ゾーンを選択できます。[タイムゾーンの選択（Select Timezone）] ポップアップ画面で、マップの上にカーソルを移動してロケーションをクリックしてタイム ゾーンを選択するか、または [タイムゾーン（Timezone）] ドロップダウン メニューからタイム ゾーンを選択します。

ステップ 5 [シャーシ要約（Chassis Summary）] ペインの [シャーシ ステータス（Chassis Status）] 領域で、次の情報を確認します。

[名前（Name）]	説明
[電源の状態（Power State）] フィールド	現在の電源状態。
[全体のサーバ ステータス（Overall Server Status）] フィールド	サーバの全体的なステータス。次のいずれかになります。 • [メモリ テストを実行中（Memory Test In Progress）]：サーバは搭載されているメモリのセルフテストを実行しています。この状態は、通常、ブート プロセスの間に発生します。 • Good • 中程度の障害（Moderate Fault） • [深刻な障害（Severe Fault）]
[温度（Temperature）] フィールド	温度ステータス。次のいずれかになります。 • Good • Fault • 重大な障害（Severe Fault） このフィールドのリンクをクリックして、詳細な温度情報を表示できます。

[名前（Name）]	説明
[全体の DIMM ステータス（Overall DIMM Status）] フィールド	メモリ モジュールの全体的なステータス。次のいずれかになります。 • Good • Fault • 重大な障害（Severe Fault） このフィールドのリンクをクリックして、詳細なステータス情報を表示できます。
[電源（Power Supplies）] フィールド	電源装置の全体的なステータス。次のいずれかになります。 • Good • Fault • 重大な障害（Severe Fault） このフィールドのリンクをクリックして、詳細なステータス情報を表示できます。
[ファン（Fans）] フィールド	電源装置の全体的なステータス。次のいずれかになります。 • Good • Fault • 重大な障害（Severe Fault） このフィールドのリンクをクリックして、詳細なステータス情報を表示できます。
[ロケータ LED（Locator LED）] フィールド	ロケータ LED がオンかオフか。
[フロント ロケータ LED（Front Locator LED）] フィールド	シャーシの前面パネル ロケータ LED がオンかオフか。 （注） このオプションを使用できるのは一部の UCS C シリーズ サーバだけです。
[全体のストレージ ステータス（Overall Storage Status）] フィールド	すべてのコントローラの全体的なステータス。次のいずれかになります。 • Good • 中程度の障害（Moderate Fault） • 重大な障害（Severe Fault）

ステップ 6 [シャーシ要約（Chassis Summary）] ペインの [サーバ使用率（Server Utilization）] 領域で、グラフで表示された次の情報を確認します。

[名前（Name）]	説明
[全体の使用率（%）（Overall Utilization (%)）] フィールド	システムの CPU、メモリ、および IO（入力/出力）の全体的なリアルタイムの使用率のパーセンテージ。
[CPU 使用率（%）（CPU Utilization (%)）] フィールド	使用可能なすべての CPU 上のシステムの CPU または計算の使用率のパーセンテージ。
[メモリ使用率（%）（Memory Utilization (%)）] フィールド	使用可能なすべてのメモリ（DIMM）チャネル上のシステムのメモリ使用率のパーセンテージ。
[IO 使用率（%）（IO Utilization (%)）] フィールド	システムの IO リソース使用率のパーセンテージ。

シャーシ インベントリ

電源のプロパティの表示

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 [インベントリ（Inventory）] をクリックします。

ステップ 3 [インベントリ（Inventory）] 作業ウィンドウで、[電源（Power Supplies）] タブをクリックし、各電源の次の情報を確認します。

名称	説明
[デバイス ID（Device ID）] カラム	電源装置ユニットの ID。
[ステータス（Status）] カラム	電源装置のステータス。
[入力（Input）] カラム	電源装置への入力（ワット単位）。
[出力（Output）] カラム	電源装置からの最大出力（ワット単位）。

名称	説明
[FW バージョン（FW Version）] カラム	電源装置のファームウェア バージョン。
[製品 ID（Product ID）] カラム	ベンダーによって割り当てられた電源の製品識別子。

Cisco VIC アダプタ プロパティの表示

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 [インベントリ（Inventory）] をクリックします。

ステップ 3 [インベントリ（Inventory）] 作業ウィンドウで、[Cisco VIC アダプタ（Cisco VIC Adapters）] タブをクリックし、次の概要を確認します。

[名前（Name）]	説明
[スロット番号（Slot Number）] カラム	アダプタが装着されている PCI スロット。
[シリアル番号（Serial Number）] カラム	アダプタのシリアル番号。
[製品 ID（Product ID）] カラム	アダプタの製品 ID。
[Cisco IMC 有効（Cisco IMC Enabled）] カラム	アダプタが Cisco IMC を管理できるかどうか。この機能は、設置されているアダプタのタイプと、その設定内容によって異なります。詳細については、使用しているサーバタイプに対応するハードウェア インストレーション ガイドを参照してください。
[説明（Description）] カラム	アダプタの説明。

SAS エクスパンダ プロパティの表示

はじめる前に

サーバの電源をオンにする必要があります。そうしないと、プロパティが表示されません。

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 [インベントリ（Inventory）] をクリックします。

ステップ 3 [インベントリ（Inventory）] 作業ウィンドウの [SAS エクスパンダ（SAS Expander）] タブをクリックし、次の情報を確認します。

[名前（Name）]	説明
[ID] カラム	エクスパンダの製品 ID。
[名前（Name）] カラム	エクスパンダの名前。
[ファームウェア バージョン（Firmware Version）] カラム	エクスパンダが使用するファームウェア バージョン。
[セカンダリ ファームウェア バージョン（Secondary Firmware Version）] カラム	エクスパンダのセカンダリ ファームウェア バージョン。
[ハードウェア リビジョン（Hardware Revision）] カラム	エクスパンダのハードウェア バージョン。
[SAS アドレス（SAS Address）] カラム	エクスパンダの SAS アドレス。
[サーバのアップ リンク速度（Server Up Link Speed）] カラム	LSI RAID コントローラで受信されるアップリンク速度。 （注） 一部の C シリーズ サーバでのみ使用できます。 （注） [SAS エクスパンダ（SAS Expander）] テーブルの右上隅にある [フィルタ（Filter）] アイコンを使用し、サーバ 1 と 2 に対して、それぞれ最大 4 つの速度レベルを表示できます。テーブル内の個々の速度を表示するには、速度フィルタの横にあるチェックマークを選択します。

SAS エクスパンダでの 6G または 12G 混合モードの有効化

このオプション（トグル ボタン）を使用して、カードでの 6 GB または 12 GB 混合モード速度のサポートを有効化または無効化できます。

（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）] メニューの [インベントリ（Inventory）] をクリックします。

ステップ 3 [インベントリ（Inventory）] 作業領域で、[SAS エクスパンダ（SAS Expander）] タブをクリックします。

ステップ 4 [SAS エクスパンダ（SAS Expander）] 作業領域で、[6G-12G 混合モードの有効化（Enable 6G-12G Mixed Mode）] をクリックします。

ステップ 5 （任意） この機能を無効化するには、[6G-12G 混合モードの無効化（Disable 6g-12G Mixed Mode）] をクリックします。

ストレージのプロパティの表示

はじめる前に

サーバの電源をオンにする必要があります。そうしないと、プロパティが表示されません。

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 [インベントリ（Inventory）] をクリックします。

ステップ 3 [インベントリ（Inventory）] 作業ウィンドウの [ストレージ（Storage）] タブをクリックし、次の情報を確認します。

[名前（Name）]	説明
[コントローラ（Controller）] フィールド	コントローラ ドライブが存在する PCIe スロット。
[PCI スロット（PCI Slot）] フィールド	コントローラ ドライブが配置されている PCIe スロットの名前。

[名前（Name）]	説明
[製品名（Product Name）] フィールド	コントローラの名前。
[シリアル番号（Serial Number）] フィールド	ストレージ コントローラのシリアル番号。
[ファームウェア パッケージ ビルド（Firmware Package Build）] フィールド	アクティブなファームウェア パッケージのバージョン番号。
[製品ID（Product ID）] フィールド	コントローラの製品 ID。
[バッテリのステータス（Battery Status）] フィールド	バッテリのステータス。
[キャッシュ メモリ サイズ（Cache Memory Size）] フィールド	キャッシュ メモリのサイズ（MB 単位）。
[状況（Health）] フィールド	コントローラのヘルス状態。

ネットワーク アダプタのプロパティの表示

はじめる前に

サーバの電源をオンにする必要があります。そうしないと、プロパティが表示されません。

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 [インベントリ（Inventory）] をクリックします。

ステップ 3 [インベントリ（Inventory）] 作業ウィンドウの [ネットワーク アダプタ（Network Adapters）] タブをクリックし、次の情報を確認します。

[名前（Name）]	説明
[スロット（Slot）] カラム	アダプタが装着されているスロット。

[名前（Name）]	説明
[製品名（Product Name）] 列	アダプタの製品名。
[インターフェイスの数（Number of Interfaces）] カラム	アダプタのインターフェイスの数。
外部イーサネットインターフェイス（External Ethernet Interfaces）	[ID]：外部イーサネット インターフェイスの ID。 [MAC アドレス（MAC Address）]：外部イーサネット インターフェイスの MAC アドレス。

第 4 章

サーバの管理

この章の内容は、次のとおりです。

サーバのブート順の管理

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からは設定していないデバイスを追加した。

（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 [実際のブート順（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 [実際のブート順（Actual Boot Order）] 領域に [NonPolicyTarget] として示されます。

（注） Cisco IMC を最新のバージョン 2.0(x) に初めてアップグレードすると、レガシー ブート順は高精度ブート順に移行されます。このプロセス中に、以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 [設定済みブート順（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、サーバの最後のレガシーブート順が保持され、それを [実際のブート順（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 では、**set boot-orderHDD,PXE** コマンドを使用して設定できます。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

はじめる前に

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 [ブート順の設定（Configure Boot Order）] タブをクリックします。

ステップ 3 [BIOS のプロパティ（BIOS Properties）] 領域で、[ブート順の設定（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 [ブート順の設定（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。

名称	説明
[ブート デバイスの追加（Add Boot Device）] テーブル	サーバのブート オプション。次のブート デバイスの 1 つ以上を追加して、選択したデバイスのパラメータを設定できます。 • ローカル HDD の追加（Add Local HDD） • PXE ブートの追加（Add PXE Boot） • SAN ブートの追加（Add SAN Boot） • iSCSI ブートの追加（Add iSCSI Boot） • [SD カードの追加（Add SD Card）] （注） このオプションを使用できるのは一部の UCS C シリーズ サーバだけです。 • USB の追加（Add USB） • 仮想メディアの追加（Add Virtual Media） • PCH ストレージの追加 • UEFI SHELL の追加 • NVME の追加 • ローカル CDD の追加
[有効/無効（Enable/Disable）] ボタン	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。
[変更（Modify）] ボタン	選択したデバイスの属性を変更します。
[削除（Delete）] ボタン	[ブート順序（Boot Order）] テーブルから選択したブート可能なデバイスを削除します。
[閉じる（Clone）] ボタン	既存のデバイス設定を新しいデバイスにコピーします。
[再適用（Re-Apply）] ボタン	最後に設定されたブート順の送信元が BIOS として表示されるとき、ブート順の設定を BIOS に再適用します。
[上へ移動（Move Up）] ボタン	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。

名称	説明
[下へ移動（Move Down）] ボタン	選択したデバイス タイプを [ブート順序（Boot Order）] テーブルで低いプライオリティに移動します。
[ブート順序（Boot Order）] テーブル	このサーバ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に表示されます。
[変更を保存（Save Changes）] ボタン	設定されているブート順に対する変更を保存するか、または以前に設定したブート順を再適用します。 Cisco IMC は、そのサーが次に再起動されるときに、設定されているブート順を BIOS に送信します。
[値のリセット（Reset Values）] ボタン	設定されたブート順の値をリセットします。
[閉じる（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。 このオプション選択すると、そのサーバが次に再起動されるときに、実際のブート順は変更されません。

ステップ 5 [変更の保存（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。

次の作業

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

はじめる前に

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 [ブート順の設定（Configure Boot Order）] タブをクリックします。

ステップ 3 [BIOS のプロパティ（BIOS Properties）] 領域で、[ブート順の設定（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 [ブート順の設定（Configure Boot Order）] ダイアログボックスで、[ブート デバイスの追加（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、[ローカル HDD の追加（Add Local HDD）] をクリックし、次のパラメータを更新します。

名称	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。
[状態（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。
[順序] 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）。
[スロット（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。
[デバイスの追加（Add Device）] ボタン	[ブート順序（Boot Order）] テーブルにデバイスを追加します。
[キャンセル（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、[PXE の追加（Add PXE）] をクリックし、次のパラメータを更新します。

名称	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。
[状態（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。
[順序] 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）。
MAC アドレス	サーバの 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 シリーズサーバだけです。
[スロット（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。
[ポート（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。

名称	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。
[状態（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。

名称	説明
[順序] 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）。
[スロット（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。
[キャンセル（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。

名称	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。
[状態（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。
[順序] 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）。
[スロット（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。
[ポート（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。

名称	説明
[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。
[キャンセル（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、[SD カードの追加（Add SD Card）] をクリックし、次のパラメータを更新します。

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

[名前（Name）]	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。
[状態（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。
[順序] 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	[ブート順序（Boot Order）] テーブルにデバイスを追加します。
[キャンセル（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、[USB の追加（Add USB）] をクリックし、次のパラメータを更新します。

[名前（Name）]	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（Name）]	説明
[サブ タイプ（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
[状態（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。
[順序] 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	[ブート順序（Boot Order）] テーブルにデバイスを追加します。
[キャンセル（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、[仮想メディア（Virtual Media）] をクリックし、次のパラメータを更新します。

[名前（Name）]	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。
[サブ タイプ（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 マップされた DVD（KVM Mapped DVD） • Cisco IMC マップされた DVD（Cisco IMC Mapped DVD） • KVM マップされた HDD（KVM Mapped HDD） • Cisco IMC マップされた HDD（Cisco IMC Mapped HDD） • KVM マップされた FDD（KVM Mapped FDD）

[名前（Name）]	説明
[状態（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。
[順序] 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	[ブート順序（Boot Order）] テーブルにデバイスを追加します。
[キャンセル（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 ストレージ（PCH Storage）] をクリックし、次のパラメータを更新します。

[名前（Name）]	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。
[状態（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。
[順序] 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（Name）]	説明
[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 の範囲の値を入力します。 • AHCI モードの SATA：1 ～ 10 の範囲の値を入力します • SWRAID モードの SATA：SATA の場合に 0、また 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 サーバだけです。
[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ます。
[キャンセル（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、[UEFI シェルの追加（Add UEFI Shell）] をクリックし、次のパラメータを更新します。

[名前（Name）]	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。
[状態（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。
[順序] 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）。
[デバイスの追加（Add Device）] ボタン	[ブート順序（Boot Order）] テーブルにデバイスを追加します。
[キャンセル（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。

システム ソフトウェア イベント：ポストセンサー、システム ファームウェア エラー。（System Software event: Post sensor, System Firmware error.）EFI ロード イメージ セキュリティ違反。（EFI Load Image Security Violation.）[0x5302] がアサートされました。（[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	タイプ
サポートされている OS	• Windows Server 2012 • Windows Server 2012 R2
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

コンポーネント	タイプ
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
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 • UCS ストレージ用 RAID コントローラ（SLOT-MEZZ） • ホスト バス アダプタ（HBA）

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 作業ウィンドウの [BIOS] タブをクリックします。

ステップ 3 [ブート順の設定（Configure Boot Order）] タブの [BIOS 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 [ブート モードの設定（Configure Boot Mode）] は変更できません。

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 [変更の保存（Save Changes）] をクリックします。

次の作業

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 作業ウィンドウの [BIOS] タブをクリックします。

ステップ 3 [BIOS プロパティ（BIOS Properties）] 領域で、[UEFI セキュア ブート（UEFI Secure Boot）] チェックボックスをオフにします。

ステップ 4 [変更の保存（Save Changes）] をクリックします。

次の作業

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。

サーバの実際のブート順の表示

サーバの実際のブート順とは、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 [ブート順の設定（Configure Boot Order）] タブをクリックします。

ステップ 3 [BIOS のプロパティ（BIOS Properties）] 領域で、[ブート順の設定（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 BIOS によって使用される実際のブート順が表示されます。

[設定済みブート デバイス（Configured Boot Devices）] セクションには、Cisco IMC を介して設定されたブート順（[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、次回そのサーバがブートしたときに、Cisco IMC がこのブート順を BIOS に送信します。基本設定では、デバイス タイプのみを指定できます。詳細設定では、スロット、ポート、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。

設定されたブート順を変更したり、以前に設定されたブート順を復元したりするには、管理者は [ブート順の設定（Configure Boot Order）] ボタンをクリックできます。これらの変更をただちに有効にするには、サーバをリブートします。[BIOS] タブを更新することで、新しいブート順を確認できます。

（注） この情報は、次回のサーバのブート時に BIOS にのみ送信されます。Cisco IMC は、設定が変更されるまで、ブート順の情報を BIOS に再送信しません。

[実際のブート デバイス（Actual Boot Devices）] セクションには、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。
- ユーザが BIOS で直接、ブート順を変更した。手動による変更を上書きするには、Cisco IMC を介して設定されたブート順を変更し、サーバをリブートします。

（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。実際にマッピングされたデバイス名とポリシー名が [実際のブート順（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検出された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 [実際のブート順（Actual Boot Order）] 領域に [NonPolicyTarget] として示されます。

ワンタイム ブート デバイスでブートするようにサーバを設定する

現在設定されているブート順序を中断することなく、次回のサーバのブートに対してのみ、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。ワン タイム ブート デバイスからサーバを起動すると、以前設定されたブート順からすべての機能のリブートが発生します。

はじめる前に

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 [ブート順の設定（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）] 領域で、[設定済みワン タイム ブート デバイス（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） 無効になっている拡張ブート デバイスで設定されている場合でも、ホストはワン タイム ブート デバイスに対して起動します。

サーバ アセット タグの作成

はじめる前に

このタスクを実行するには、user または admin 権限で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）] メニューの [サマリー（Summary）] をクリックします。

ステップ 3 [サーバのプロパティ（Server Properties）] 領域で、[アセット タグ（Asset Tag）] フィールドを更新します。

ステップ 4 [変更の保存（Save Changes）] をクリックします。

電力ポリシーの設定

電力の制限

重要 この項が適用されるのは、一部の UCS C シリーズ サーバだけです。

電力制限によって、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。電力制限オプションを有効にすると、システムは電力消費をモニタし、割り当てられた電力制限未満の値に電力を維持します。サーバが電力制限を維持できない場合や、プラットフォームの電力を修正用の時間内に指定された電力制限に戻すことができない場合は、電力制限によって、[電力プロファイル（Power Profile）] 領域の [アクション（Action）] フィールドでユーザが指定したアクションが実行されます。

電力制限が有効になると、定義された属性を使用して、標準または高度な電力プロファイルを持つ複数の電力プロファイルを設定できます。標準の電力プロファイルを選択した場合は、電力制限、修正用時間、是正措置、一時停止期間、ハード キャッピング、およびポリシー状態（有効な場合）を設定できます。高度な電力プロファイルを選択した場合は、標準の電力プロファイルの属性に加えて、ドメイン固有の電力制限、安全なスロットル レベル、周囲温度ベースの電力制限属性も設定できます。

（注） 次の変更は、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、最初のホストの電源オン時に電力特性評価が自動的に実行されます。後続の特性評価は、「電力特性評価の実行」の項の説明に従って起動された場合にのみ実行されます。
- また、サーバの電源が再投入されたときに CPU または DIMM の設定に対する変更がある場合、電力特性評価は最初のホストのブート時に自動的に実行されます。PCIe アダプタ、GPU または HDD などの他のハードウェアの変更の場合は、電力特性評価は実行されません。特性化される電力範囲は、ホストの電源の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 [電力制限の設定（Power Cap Configuration）] タブの [電力特性評価の実行（Run Power Characterization）] オプションを使用すると、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 サーバだけです。

はじめる前に

このタスクを実行するには、admin 権限で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）] メニューの [電源管理（Power Management）] をクリックします。

ステップ 3 [電力制限の設定（Power Cap Configuration）] タブで、[電力特性評価の実行（Run Power Characterization）] リンクをクリックします。

現在の電源の状態に応じて、ホストの電源がオンにされるか、または再起動されるかを通知する確認メッセージ 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。

- [実行していません（Not Run）]：初期設定へのリセット以降に電力特性評価がまったく実行されていない場合。
- [実行中（Running）]：電力特性評価プロセスが進行中の場合。
- [完了（Completed Successfully）]：電力特性評価が正常に実行された場合。
- [デフォルト値を使用（Using Defaults）]：電力特性評価の実行後、システムが有効な値を取得できない場合、システムは電力制限に推奨される最大および最小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 [推奨される電力キャップ（Recommended Power Cap）] 領域に読み込まれます。

電力制限の有効化

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 サーバだけです。

はじめる前に

- このタスクを実行するには、admin 権限で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）] メニューの [電源管理（Power Management）] をクリックします。

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

（注） これは、電力制限を有効または無効にするグローバル オプションです。電力プロファイルを設定するには、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 [変更の保存（Save Changes）] をクリックします。

電力プロファイル

複数のプロファイルを設定し、属性を設定できます。これらのプロファイルは、Web UI または CLI を使用して設定します。Web UI では、プロファイルは [電力の制限（Power Capping）] 領域の下にリストされます。CLI で、power-cap-config**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）] : 電力制限ポリシー、フェールセーフ電力制限ポリシー、周囲温度ベースの電力制限ポリシーなどのさまざまな属性を設定できます。

標準の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 サーバだけです。

はじめる前に

- 電力制限をイネーブルにする必要があります。
- このタスクを実行するには、admin 権限で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）] メニューの [電源管理（Power Management）] をクリックします。

ステップ 3 [電力プロファイル（Power Profiles）] 領域で、次のフィールドに値を入力します。

[名前（Name）]	**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。
[プロファイルの有効化（Enable Profile）] チェックボックス	編集用に電力プロファイルを有効にします。
[スロットルを許可（Allow Throttle）] チェックボックス	オンにすると、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に、CPU スロットリング状態（T-states）やメモリ帯域幅スロットリングなどのより積極的な電力管理メカニズムを使用するようにプロセッサに強制します。

[名前（Name）]	説明
[修正用時間（Correction Time）] フィールド	[アクション（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る最小修正用時間は 1 秒ですが、DPST-1400AB および DPST-1200DB PSU モデルの場合は、サポートされる最小修正用時間が 3 秒になります。
[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）] : Cisco IMC SEL にイベントを記録します。 • [アラートおよびシャットダウン（Alert and Shutdown）] : イベントを Cisco IMC SEL に記録し、ホストをグレースフル シャットダウンします。
[電力上限（Power Capping）] チェックボックス	サーバの電力制限。 指定された範囲内の電力（ワット単位）を入力します。
[ハードキャップの設定（Set Hard Cap）] チェックボックス	オンにした場合、設定した電力制限値を超えたプラットフォームの消費が発生しないようにされます。プラットフォームの電力消費は、設定された電力キャップ値未満の安全なオフセットマージンで維持されます。

ステップ 4 [変更の保存（Save Changes）] をクリックします。

高度な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 サーバだけです。

はじめる前に

- 電力制限をイネーブルにする必要があります。
- このタスクを実行するには、admin 権限で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）] メニューの [電源管理（Power Management）] をクリックします。

ステップ 3 [電力制限の設定（Power Cap Configuration）] タブの [電力プロファイル（Power Profiles）] テーブルから、[高度な（Advanced）] プロファイルを選択します。
標準のプロファイル設定に加えて、[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 [周囲温度ベースの電力制限（Ambient Temperature Based Power Capping）] 領域が表示されます。

ステップ 4 [ドメイン固有の電力制限（Domain Specific Power Limit）] 領域で、次のフィールドに値を入力します。

名称	説明
[CPU] フィールド	CPU の電力制限。 指定された範囲内の電力（ワット単位）を入力します。
[メモリ（Memory）] フィールド	メモリの電力制限。 指定された範囲内の電力（ワット単位）を入力します。
[プラットフォーム（Platform）] フィールド	プラットフォームの電力制限。 指定された範囲内の電力（ワット単位）を入力します。

ステップ 5 [一時停止期間（Suspend Period）] 領域で、[設定（Configure）] をクリックし、特定の時間帯と日に対して一時停止期間を設定します。

ステップ 6 [安全スロットル レベル（Safe Throttle Level）] 領域で、次のフィールドに値を入力します。

[名前（Name）]	説明
[フェールセーフ タイムアウト（Failsafe Timeout）] フィールド	プラットフォームまたは CPU の電力読み取り不足などの内部エラーにより電力制限が影響を受ける場合に適用される安全なスロットルポリシー。 秒単位で値を入力します

[名前（Name）]	説明
[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 ～ 100 のパーセンテージです。

ステップ 7 [周囲温度ベースの電力制限（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（Name）]	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）の温度センサー値（摂氏単位）。 （注） プラットフォームのインレット部の温度が指定された上限を超えると、システムは電力制限の上限として温度による電力制限値を使用します。
[温度による電力制限（Thermal Power Limit）] フィールド	維持される電力制限（ワット単位）。

ステップ 8 [変更の保存（Save Changes）] をクリックします。

電力プロファイルをデフォルトにリセット

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 サーバだけです。

はじめる前に

このタスクを実行するには、admin 権限で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）] メニューの [電源管理（Power Management）] をクリックします。

ステップ 3 [電力プロファイル（Power Profiles）] 領域で、[プロファイルをデフォルトにリセット（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の設定が工場出荷時のデフォルト値にリセットされ、電力制限が無効になります。

ステップ 4 [変更の保存（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、ホストの電源が投入された時間またはホストが起動された時間から開始されます。この機能により、プラットフォーム、CPU およびメモリ領域の電力消費の統計情報が収集され、収集されている期間中の最小、最大、および平均の読み取り値が提供されます。これらの読み取り値は、その領域の電力消費の傾向を計算するために使用できます。Cisco IMC は、これらの電力消費の統計値を収集して保存し、さまざまな時間帯（1 時間、1 日、1 週間など）でグラフを作成します。

（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）] メニューの [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。
次の表のように、最後にリブートし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（Name）]	説明
モニタリング期間（Monitoring Period）	最後にリブートされてからシステムによって使用される電力をモニタリングする時間。 モニタリング期間は、Day HH:MM:SS の形式で表示されます。

ステップ 5 [プラットフォーム（Platform）] 領域で、次の情報を確認します。

[名前（Name）]	説明
現在（Current）	サーバ、CPU、およびメモリによって現在使用されている電力（ワット単位）。
[最小（Minimum）]	最後にリブートされてからサーバ、CPU、およびメモリが使用した最小ワット数。

[名前（Name）]	説明
[最大数（Maximum）]	最後にリブートされてからサーバ、CPU、およびメモリが使用した最大ワット数。
[平均（Average）]	定義された期間にわたってサーバ、CPU、およびメモリが使用した平均電力量。

ステップ 6 [CPU] 領域で、次の情報を確認します。

[名前（Name）]	説明
現在（Current）	現在 CPU によって使用されている電力（ワット単位）。
最小	最後にリブートされてから CPU が使用した最小ワット数。
最大数	最後にリブートされてから CPU が使用した最大ワット数。
平均（Average）	定義された期間にわたってサーバ、CPU、およびメモリが使用した平均電力量。

ステップ 7 [メモリ（Memory）] 領域で、次の情報を確認します。

[名前（Name）]	説明
現在（Current）	現在メモリによって使用されている電力（ワット単位）。
最小	最後にリブートされてからメモリが使用した最小ワット数。
最大数	最後にリブートされてからメモリが使用した最大ワット数。
平均（Average）	定義された期間にわたってメモリが使用した平均電力量。

ステップ 8 [グラフプロパティ（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（Name）]	説明
グラフの設定（Chart Settings）	グラフのプロパティとグラフでのデータ表示方法を設定できます。

[名前（Name）]	説明
電力統計情報とサーバ使用率データのダウンロード（Download Power Statistics and Server Utilization Data）	電力統計情報とホストサーバの使用率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） すでにダウンロードされている統計情報ファイルのファイルサイズが 256 KB 未満の場合に、ダウンロードを行うと、別のファイルのセット（電力統計情報用のファイルとホストサーバ使用率用のファイル）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。

[名前（Name）]	説明
[グラフ（Chart）] ドロップダウン リスト	選択した期間のすべてのサーバから電力消費の傾向を収集することができます。次のいずれかになります。 • [過去 1 時間（Last One Hour）] : 5 分おきのグラフを作成します。 • [過去 1 日（Last One Day）] : 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（Last One Week）] : 毎日のグラフを作成します。
[コンポーネント（Component）] ドロップダウン リスト	選択した期間にわたる電力消費を確認するコンポーネント。次のいずれかになります。 • プラットフォーム • [CPU] • [メモリ（Memory）] • すべて（All）
[プロット（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。
[グラフ/テーブル（Chart/Table）] ビュー（カーソルを重ねると表示されます）	電力モニタリングの概要を [グラフ（Chart）] ビューと [テーブル（Table）] ビューのどちらで表示するかを選択します。

[名前（Name）]	説明
[グラフ タイプ（Chart Type）]（カーソルを重ねると表示されます）	表示するグラフのタイプを選択します。次のいずれかを選択できます。 • [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。 • [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。
[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。
[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。
[最大（Maximum）] 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大ワット数がグラフに表示されます。
[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。

グラフでの電力統計情報の表示

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 サーバだけです。

はじめる前に

- 電力制限をイネーブルにする必要があります。
- このタスクを実行するには、admin 権限で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）] メニューの [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、電力消費の詳細を表示するには、グラフ、コンポーネントを確認して更新します。

[名前（Name）]	**説明**
[グラフ（Chart）] ドロップダウン リスト	選択した期間のすべてのサーバから電力消費の傾向を収集することができます。次のいずれかになります。 • [過去 1 時間（Last One Hour）]：5 分おきのグラフを作成します。 • [過去 1 日（Last One Day）]：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（Last One Week）]：毎日のグラフを作成します。
[コンポーネント（Component）] ドロップダウン リスト	選択した期間にわたる電力消費を確認するコンポーネント。次のいずれかになります。 • プラットフォーム • [CPU] • [メモリ（Memory）] • すべて（All）
[最大（Maximum）] 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大ワット数がグラフに表示されます。
[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。

[名前（Name）]	説明
[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。
[プロット（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。

電力読み取りグラフには、選択した期間の各種コンポーネントの電力消費値が示されます。これらの電力消費値は、ホストの電源がオンになった時刻からキャプチャされます。電力プロファイルを有効にすると、電力制限が赤い線でグラフに示されます。このプロットを使用して、システムの電力消費の傾向を判断できます。特定のドメインの設定された電力上限値を表示するには、これらの傾向線の上にマウスを移動します。

標準プロファイルを選択した場合、傾向線は電力制限を表します。アドバンス プロファイルを選択した場合、傾向線は電力プロファイル設定に応じた CPU、メモリ、およびプラットフォームの電力制限を表します。

（注） これらの傾向線は、プロファイルが [電力制限の設定（Power Cap Configuration）] タブで無効になっている場合は表示されません。

ステップ 5 [変更の保存（Save Changes）] をクリックします。

電力統計情報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 サーバだけです。

はじめる前に

このタスクを実行するには、admin 権限で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）] メニューの [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、[電力統計情報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） すでにダウンロードされている統計情報ファイルのファイル サイズが 256 KB 未満の場合に、ダウンロードを行うと、別のファイルのセット（電力統計情報用のファイルとホスト サーバ使用率用のファイル）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、サーバに電力を復元する方法が決定されます。

はじめる前に

このタスクを実行するには、admin 権限で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 作業ウィンドウの [電源ポリシー（Power Policies）] タブをクリックします。

ステップ 3 [電力復元ポリシー（Power Restore Policy）] 領域で、次のフィールドを更新します。

[名前（Name）]	**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、サーバは通常どおりに起動できます。サーバ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）]：サーバが再起動し、システムは電源損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 [変更の保存（Save Changes）] をクリックします。

ファン ポリシーの設定

サーバ設定およびサーバ 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。

はじめる前に

このタスクを実行するには、admin 権限で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 作業ウィンドウの [電源ポリシー（Power Policies）] タブをクリックします。

ステップ 3 [設定済みファン ポリシー（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。次のいずれかを設定できます。

[名前（Name）]	説明
[ファン ポリシー（Fan Policy）] ドロップダウン リスト	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構成に使用できます。 この設定により、ファン速度は、[平衡化（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 サーバだけです。 • [低電力（Low Power）]：これはデフォルトのポリシーです。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）]：この設定は、60 ～ 85% のファン速度を必要とするサーバ構成で使用できます。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に最適です。このポリシーで設定される最小ファン速度はサーバごとに異なりますが、およそ 50 ～ 85% の範囲です。 • [最大電力（Maximum Power）]：この設定は、70 ～ 100% の範囲の非常に高いファン速度を必要とするサーバ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。このポリシーで設定される最小ファン速度はサーバごとに異なりますが、およそ 70 ～ 100% の範囲です。

[名前（Name）]	説明
[適用済みファン ポリシー（Applied Fan Policy）] フィールド	サーバで実行されているファンの実際の速度。 設定されたファン ポリシーが有効になっていない場合は、[なし（N/A）] と表示されます。設定されたファン ポリシーは、サーバの電源が入り、POST が完了すると有効になります。

[設定ステータス（Configuration Status）] フィールド	ファン ポリシーの設定ステータス。次のいずれかになります。
	• [成功（SUCCESS）] : 設定したファン速度が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。
	• [保留中（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。これは次のいずれかが原因として考えられます。
	  • 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。

ステップ 4 [変更の保存（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 エラーを検出した場合、DIMM は不良と判断されます。不良と判別された 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 エラーが検出された 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 は、修正不可能なエラーが発生した場合にのみマッピング解除またはブラックリスト化されます。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） DIMM は、16000 の修正可能なエラーの場合はマッピング解除またはブラックリスト化されません。

DIMM のブラックリストのイネーブル化

はじめる前に

- 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）] メニューの [インベントリ（Inventory）] をクリックします。

ステップ 3 [インベントリ（Inventory）] ペインの [メモリ（Memory）] タブをクリックします。

ステップ 4 [メモリ（Memory）] ペインの [DIMM のブラックリスト化（DIMM Black Listing）] 領域で、[DIMM のブラックリストのイネーブル化（Enable DIMM Black List）] チェックボックスをオンにします。

Configuring BIOS Settings

はじめる前に

このタスクを実行するには、admin 権限で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 次のタブを更新します。

表 *1*：*[I/O]* タブの *BIOS* のパラメータ

[名前（Name）]	説明
[ホストを即座にリブート（Reboot Host Immediately）] チェックボックス	オンにすると、ホスト サーバが直ちに再起動されます。このチェックボックスは、変更を保存してからオンにする必要があります。
[レガシー USB サポート（Legacy USB Support）] ドロップダウン リスト	システムでレガシーUSBデバイスをサポートするかどうか。次のいずれかになります。 • [無効（Disabled）]：USBデバイスは、EFIアプリケーションでのみ使用できます。 • [有効（Enabled）]：レガシー USB のサポートは常に使用できます。
[ダイレクト IO への Intel VT（Intel VT for directed IO）] ドロップダウン リスト	プロセッサで Intel Virtualization Technology（VT）を使用するかどうか。このテクノロジーでは、1 つのプラットフォームで、複数のオペレーティング システムとアプリケーションをそれぞれ独立したパーティション内で実行できます。次のいずれかになります。 • [無効（Disabled）]：プロセッサでの仮想化を禁止します。 • [有効（Enabled）]：プロセッサで、複数のオペレーティング システムをそれぞれ独立したパーティション内で実行できます。 （注） このオプションを変更した場合は、設定を有効にするためにサーバの電源を再投入する必要があります。

[名前（Name）]	説明
[Intel VTD coherency サポート（Intel VTD coherency support）] ドロップダウン リスト	プロセッサで Intel VT-d Coherency をサポートするかどうか。次のいずれかになります。 • [無効（Disabled）]：プロセッサでコヒーレンシをサポートしません。 • [有効（Enabled）]：プロセッサで VT-d Coherency を必要に応じて使用します。
[Intel VTD ATS サポート（Intel VTD ATS support）] ドロップダウン リスト	プロセッサで Intel VT-d Address Translation Services（ATS）をサポートするかどうか。次のいずれかになります。 • [無効（Disabled）]：プロセッサで ATS をサポートしません。 • [有効（Enabled）]：プロセッサで VT-d ATS を必要に応じて使用します。
[すべてのオンボード LOM Oprom（All Onboard LOM Oprom）] ドロップダウン リスト	オプション ROM がすべての LOM ポートで使用できるかどうか。次のいずれかになります。 • [無効（Disabled）]：すべてのポートでオプション ROM を無効にします。 • [有効（Enabled）]：すべてのポートでオプション ROM を有効にします。
[オンボード LOM ポート 0 Oprom（Onboard LOM Port0 Oprom）] ドロップダウン リスト	オプション ROM が LOM ポート 0 で使用できるかどうか。次のいずれかになります。 • [無効（Disabled）]：LOM ポート 0 でオプション ROM を使用できません。 • [有効（Enabled）]：LOM ポート 0 でオプション ROM を使用できます。
[オンボード LOM ポート 1 Oprom（Onboard LOM Port1 Oprom）] ドロップダウン リスト	オプション ROM が LOM ポート 1 で使用できるかどうか。次のいずれかになります。 • [無効（Disabled）]：LOM ポート 1 でオプション ROM を使用できません。 • [有効（Enabled）]：LOM ポート 1 でオプション ROM を使用できます。

[名前（Name）]	説明
[PCIe スロット *n* Oprom（Pcie Slot n Oprom）] ドロップダウンリスト	サーバが *n* で指定した PCIe カード スロットにあるオプション ROM を使用できるかどうか。次のいずれかになります。 • [無効（Disabled）]：スロット *n* のオプション ROM は使用できません。 • [有効（Enabled）]：スロット *n* のオプション ROM は使用可能です。
[MLOM Oprom] ドロップダウンリスト	このオプションでは、MLOM スロットに接続された PCIe アダプタのオプション ROM の実行を制御することができます。次のいずれかになります。 • [無効（Disabled）]：MLOM スロットに接続されている PCIe アダプタのオプション ROM を実行しません。 • [有効（Enabled）]：MLOM スロットに接続されている PCIe アダプタのオプション ROM を実行します。
[HBA Oprom] ドロップダウンリスト	このオプションでは、HBA スロットに接続された PCIe アダプタのオプション ROM の実行を制御することができます。次のいずれかになります。 • [無効（Disabled）]：HBA スロットに接続されている PCIe アダプタのオプション ROM を実行しません。 • [有効（Enabled）]：HBA スロットに接続されている PCIe アダプタのオプション ROM を実行します。
[フロント NVME1 Oprom（Front NVME1 Oprom）] ドロップダウン リスト	このオプションでは、SSD:NVMe1 スロットに接続された PCIe アダプタのオプション ROM の実行を制御することができます。次のいずれかになります。 • [無効（Disabled）]：SSD:NVMe1 スロットに接続されている PCIe アダプタのオプション ROM を実行しません。 • [有効（Enabled）]：SSD:NVMe1 スロットに接続されている PCIe アダプタのオプション ROM を実行します

[名前（Name）]	説明
[フロントNVME2 Oprom（Front NVME2 Oprom）] ドロップダウン リスト	このオプションでは、SSD:NVMe2 スロットに接続された PCIe アダプタのオプションROMの実行を制御することができます。次のいずれかになります。 • [無効（Disabled）]：SSD:NVMe2 スロットに接続されている PCIe アダプタのオプション ROM を実行しません。 • [有効（Enabled）]：SSD:NVMe2 スロットに接続されている PCIe アダプタのオプション ROM を実行します
[HBA リンク速度（HBA Link Speed）] ドロップダウン リスト	このオプションを使用すると、PCIe HBA スロットに装着されているアダプタ カードの最大速度を制限できます。次のいずれかになります。 • [無効（Disabled）]：最大速度は制限されません。 • [自動（Auto）]：システムは許容最大速度を選択します。 • [GEN1]：最大 2.5GT/s（ギガトランスファー/秒）までの速度が許可されます。 • [GEN2]：最大 5GT/s までの速度が許可されます。 • [GEN3]：最大 8GT/s までの速度が許可されます。
[MLOM リンク速度（MLOM Link Speed）] ドロップダウン リスト	このオプションを使用すると、PCIe MLOM スロットに装着されているアダプタ カードの最大速度を制限できます。次のいずれかになります。 • [無効（Disabled）]：最大速度は制限されません。 • [自動（Auto）]：システムは許容最大速度を選択します。 • [GEN1]：最大 2.5GT/s（ギガトランスファー/秒）までの速度が許可されます。 • [GEN2]：最大 5GT/s までの速度が許可されます。 • [GEN3]：最大 8GT/s までの速度が許可されます。

[名前（Name）]	説明
[PCIe スロット *n* リンク速度（PCIe Slot n Link Speed）] ドロップダウン リスト	システム IO コントローラ *n*（SIOCn）アドオン スロット（*n* によって示される）のリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効であり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：リンク速度は第 2 世代まで到達可能です。 • [GEN3]：リンク速度は第 3 世代まで到達可能です。
[フロント NVME1 リンク速度（Front NVME1 Link Speed）] ドロップダウン リスト	NVMe フロント スロット 1 のリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効であり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：リンク速度は第 2 世代まで到達可能です。 • [GEN3]：リンク速度は第 3 世代まで到達可能です。
[フロント NVME2 リンク速度（Front NVME2 Link Speed）] ドロップダウン リスト	NVMe フロント スロット 2 のリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効であり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：リンク速度は第 2 世代まで到達可能です。 • [GEN3]：リンク速度は第 3 世代まで到達可能です。

[名前（Name）]	説明
[リア NVME1 リンク速度（Rear NVME1 Link Speed）] ドロップダウン リスト	NVMe 背面のスロット 1 のリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効であり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：リンク速度は第 2 世代まで到達可能です。 • [GEN3]：リンク速度は第 3 世代まで到達可能です。
[リア NVME2 リンク速度（Rear NVME2 Link Speed）] ドロップダウン リスト	NVMe 背面のスロット 2 のリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効であり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：リンク速度は第 2 世代まで到達可能です。 • [GEN3]：リンク速度は第 3 世代まで到達可能です。
[VGA 優先順位（VGA Priority）] ドロップダウン リスト	システムに複数の VGA デバイスがある場合は、VGA グラフィックスデバイスのプライオリティを設定できます。次のいずれかになります。 • [オンボード（OnBoard）]：オンボード VGA デバイスが優先されます。BIOS ポスト画面および OS ブートはオンボード VGA ポート経由で駆動されます。 • [オフボード（OffBoard）]：PCIE グラフィックス アダプタが優先されます。BIOS ポスト画面および OS ブートは外部グラフィックス アダプタ ポート経由で駆動されます。 • [オンボードを無効（OnBoardDisabled）]：PCIE グラフィックス アダプタが優先され、オンボード VGA デバイスは無効になります。オンボード VGA が無効の場合、vKVM は機能しません。

[名前（Name）]	説明
[P-SATA OptionROM] ドロップダウン リスト	PCH SATA オプション ROM モードを選択できます。次のいずれかになります。 • [LSI SW Raid]：SATA コントローラと sSATA コントローラを LSI SW Raid の raid モードに設定します。 • [無効（Disabled）]：SATA コントローラと sSATA コントローラを無効にします。
[M2.SATA OptionROM] ドロップダウン リスト	Serial Advanced Technology Attachment（SATA）ソリッド ステート ドライブ（SSD）の動作モード。次のいずれかになります。 • [AHCI]： SATA コントローラと sSATA コントローラの両方を AHCI モードに設定します。 • [LSI SW Raid]：SATA コントローラと sSATA コントローラを LSI SW Raid の raid モードに設定します。 • [無効（Disabled）]：SATA コントローラと sSATA コントローラを無効にします。
[リア USB ポート（USB Port Rear）] ドロップダウン リスト	背面パネルの USB デバイスが有効か無効か。次のいずれかになります。 • [無効（Disabled）]：背面パネルの USB ポートを無効にします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されません。 • [有効（Enabled）]：背面パネルの USB ポートを有効にします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されます。
[フロント USB ポート（USB Port Front）] ドロップダウン リスト	前面パネルの USB デバイスが有効か無効か。次のいずれかになります。 • [無効（Disabled）]：前面パネルの USB ポートを無効にします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されません。 • [有効（Enabled）]：前面パネルの USB ポートを有効にします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されます。

[名前（Name）]	説明
[内部 USB ポート（USB Port Internal）] ドロップダウン リスト	内部USBデバイスが有効か無効か。次のいずれかになります。 • [無効（Disabled）]：内部の USB ポートを無効にします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されません。 • [有効（Enabled）]：内部の USB ポートを有効にします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されます。
[KVM USB ポート（USB Port KVM）] ドロップダウン リスト	KVM ポートが有効か無効か。次のいずれかになります。 • [無効（Disabled）]：KVM キーボードおよびマウス デバイスを無効にします。キーボードとマウスは KVM ウィンドウで機能しなくなります。 • [有効（Enabled）]：KVM キーボードおよびマウス デバイスを有効にします。
[SD カード USB ポート（USB Port SD Card）] ドロップダウン リスト	SD カードが有効か無効か。次のいずれかになります。 • [無効（Disabled）]：SD カードのポートを無効にします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されません。 • [有効（Enabled）]：SD カードのポートを有効にします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されます。
[IPV6 PXE サポート（IPV6 PXE Support）] ドロップダウン リスト	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。 • [無効（disabled）][無効（Disabled）]：IPV6PXE のサポートは利用できません。 • [有効（enabled）][有効（Enabled）]：IPV6PXE のサポートを常に利用できます。

表 *2* : *[*サーバ管理（***Server Management***）*]* タブの ***BIOS*** パラメータ

[名前（Name）]	説明
[ホストを即座にリブート（Reboot Host Immediately）] 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。
[OS ブート ウォッチドッグ タイマー ポリシー（OS Boot Watchdog Timer Policy）] ドロップダウン リスト	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。 • [電源オフ（Power Off）] : 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。 • [リセット（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、サーバはリセットされます。 （注） このオプションは [OS ブート ウォッチドッグ タイマー（OS Boot Watchdog Timer）] を有効にした場合にのみ適用されます。
[OS ウォッチドッグ タイマー（OS Watchdog Timer）] ドロップダウン リスト	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。 • [無効（Disabled）] : 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（Enabled）] : サーバ ブートにかかる時間をウォッチドッグ タイマーで追跡します。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 IMC 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。

[名前（Name）]	説明
[OS ブート ウォッチドッグ タイマー タイムアウト（OS Watchdog Timer Timeout）] ドロップダウン リスト	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。次のいずれかになります。 • [5 分（5 Minutes）] : OS ウォッチドッグ タイマーは、ブートが開始されてから 5 分後に期限が切れます。 • [10 分（10 Minutes）] : OS ウォッチドッグ タイマーは、ブートが開始されてから 5 分後に期限が切れます。 • [15 分（15 Minutes）] : OS ウォッチドッグ タイマーは、ブートが開始されてから 5 分後に期限が切れます。 • [20 分（20 Minutes）] : OS ウォッチドッグ タイマーは、ブートが開始されてから 5 分後に期限が切れます。 （注） このオプションは [OS ブート ウォッチドッグ タイマー（OS Boot Watchdog Timer）] を有効にした場合にのみ適用されます。

[名前（Name）]	説明
[ボー レート（Baud Rate）] ドロップダウン リスト	シリアル ポートの伝送速度として使用されるボー レート。[コンソール リダイレクション（Console Redirection）] を無効にした場合は、このオプションを使用できません。次のいずれかになります。 • [9.6k]：9,600 ボー レートが使用されます。 • [19.2k]：19,200 ボー レートが使用されます。 • [38.4k]：38,400 ボー レートが使用されます。 • [57.6k]：57,600 ボー レートが使用されます。 • [115.2k]：115,200 ボー レートが使用されます。 この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。
[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 リダイレクションに使用できるようにします。OS が起動した後は、コンソール リダイレクトは関係ありません。次のいずれかになります。 • [シリアル ポート A（Serial Port A）]：POST 中にシリアル ポート A でコンソール リダイレクションを有効にします。 • [シリアル ポート B（Serial Port B）]：POST 中にシリアル ポート B でコンソール リダイレクションを有効にします。 • [無効（Disabled）]：POST 中にコンソール リダイレクションは発生しません。

[名前（Name）]	説明
[CDN コントロール（CDN Control）] ドロップダウン リスト	イーサネット ネットワークの命名規則が Consistent Device Naming（CDN）または従来の命名規則に従うかどうか。次のいずれかになります。 • [無効（Disabled）]：VIC カードの CDN サポートが無効になります • [有効（Enabled）]：VIC カードの CDN サポートが有効になります。
[FRB 2 タイマー（FRB 2 Timer）] ドロップダウン リスト	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 Cisco IMC によって FRB2 タイマーが使用されるかどうか。次のいずれかになります。 • [無効（Disabled）]：FRB2 タイマーは使用されません。 • [有効（Enabled）]：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。
[フロー制御（Flow Control）] ドロップダウン リスト	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。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。 • [なし（None）]：フロー制御は使用されません。 • [RTS/CTS]：RTS/CTS がフロー制御に使用されます。 （注） この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。

[名前（Name）]	説明
[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。 • [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。

表 *3* : *[*セキュリティ（***Security***）*]* タブの ***BIOS*** パラメータ

[名前（**Name**）]	説明
[ホストを即座にリブート（Reboot Host Immediately）] 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。**
[信頼されたプラットフォーム モジュールのサポート（Trusted Platform Module Support）] ドロップダウン リスト	信頼されたプラットフォーム モジュール（TPM）は、主に暗号キーを使用する基本的なセキュリティ関連機能を提供するように設計されたマイクロチップです。このオプションを使用すると、システムの TPM セキュリティ デバイス サポートを制御できます。次のいずれかを設定できます。 • [無効（Disabled）] : サーバは TPM を使用しません。 • [有効（Enabled）] : サーバは TPM を使用します。 （注） オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせください。
[電源オン パスワード（Power On Password）] ドロップダウン リスト	このトークンでは、F2 BIOS 設定を使用する前に BIOS パスワードを設定する必要があります。有効にすると、IO 設定、BIOS セットアップ、BIOS を使用したオペレーティング システムへの起動など、BIOS 機能にアクセスする前にパスワードを検証する必要があります。次のいずれかを設定できます。 • [無効（Disabled）] : サポートはディセーブルになっています。 • [有効（Enabled）] : サポートはイネーブルになっています。

表 *4* : *[プロセッサ（Processor）]タブの BIOS パラメータ*

[名前（Name）]	説明
[Intel Virtualization Technology] ドロップダウンリスト	プロセッサで Intel Virtualization Technology（VT）を使用するかどうか。このテクノロジーでは、1 つのプラットフォームで、複数のオペレーティング システムとアプリケーションをそれぞれ独立したパーティション内で実行できます。次のいずれかになります。 • [無効（Disabled）] : プロセッサでの仮想化を禁止します。 • [有効（Enabled）] : プロセッサで、複数のオペレーティング システムをそれぞれ独立したパーティション内で実行できます。
[拡張 APIC（Extended APIC）] ドロップダウンリスト	拡張 APIC サポートを有効または無効にできます。次のいずれかになります。 • [有効（Enabled）] : APIC サポートを有効にします • [無効（Disabled）] : APIC サポートを無効にします。
[プロセッサ C1E（Processor C1E）] ドロップダウン リスト	C1 ステートに入ったときに、CPU が最小周波数に移行するかどうか。次のいずれかになります。 • [無効（Disabled）] : CPU は C1 ステートでも引き続き最大周波数で動作します。 • [有効（Enabled）] : CPU は最小周波数に移行します。このオプションでは C1 ステートで節約される電力量が最大になります。 （注） このオプションを使用できるのは一部の C シリーズ サーバだけです。

[名前（Name）]	説明
[プロセッサ C6 レポート（Processor C6 Report）] ドロップダウン リスト	BIOS からオペレーティング システムに C6 レポートを送信するかどうか。OS はレポートを受信すると、プロセッサを電力量の少ない C6 状態に移行してエネルギー使用量を減らし、最適なプロセッサ パフォーマンスを維持できます。次のいずれかになります。 • [無効（Disabled）] : BIOS から C6 レポートを送信しません。 • [有効（Enabled）] : BIOS から C6 レポートを送信し、OS がプロセッサを電力量の少ない C6 状態に移行できるようにします。 （注） [CPUPowerManagement] を [カスタム（Custom）] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。 （注） このオプションを使用できるのは一部の C シリーズ サーバだけです。
[XD ビット（Execute Disable Bit）] ドロップダウンリスト	アプリケーション コードを実行できる場所を指定するために、サーバのメモリ領域を分類します。この分類の結果、悪意のあるワームがバッファにコードを挿入しようとした場合、プロセッサでコードの実行を無効にします。この設定は、損害、ワームの増殖、および特定クラスの悪意のあるバッファ オーバーフロー攻撃を防止するのに役立ちます。次のいずれかになります。 • [無効（Disabled）] : プロセッサでメモリ領域を分類しません。 • [有効（Enabled）] : プロセッサでメモリ領域を分類します。 （注） オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせください。

[名前（Name）]	説明
[Intel Turbo Boost Tech] ドロップダウン リスト	プロセッサで Intel Turbo Boost Technology を使用するかどうか。Turbo Boost では、仕様よりも低い電力、温度、または電圧でプロセッサが動作していると、自動的にプロセッサの周波数が上がります。次のいずれかになります。 • [無効（Disabled）]：プロセッサの周波数は自動的には上がりません。 • [有効（Enabled）]：必要に応じてプロセッサで Turbo Boost Technology が利用されます。 （注） [CPUPowerManagement] を [カスタム（Custom）] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。
[Enhanced Intel SpeedStep Tech] ドロップダウン リスト	プロセッサで Enhanced Intel SpeedStep Technology を使用するかどうか。SpeedStep では、プロセッサの電圧やコア周波数をシステムが動的に調整します。SpeedStep を有効にすると、平均電力消費量と平均熱発生量が減少する可能性があります。次のいずれかになります。 • [無効（Disabled）]：プロセッサの電圧または周波数を動的に調整しません。 • [有効（Enabled）]：プロセッサで Enhanced Intel SpeedStep Technology が使用され、サポートされているすべてのスリープ状態でさらに電力を節約することが可能になります。 オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。 （注） [CPUPowerManagement] を [カスタム（Custom）] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。

[名前（Name）]	説明
[Intel HyperThreading Tech] ドロップダウンリスト	プロセッサで Intel Hyper-Threading Technology を使用するかどうか。Hyper-Threading 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。 • [無効（Disabled）] : プロセッサでのハイパースレッディングを禁止します。 • [有効（Enabled）] : プロセッサでの複数スレッドの並列実行を許可します。
[ワークロード設定（Workload Configuration）] ドロップダウン リスト	この機能を使用すると、ワークロードを最適化できます。オプションは[バランス（Balanced）] と [I/O に依存（I/O Sensitive）] です。 • NUMA • UMA
[コア マルチプロセッシング（Core MultiProcessing）] ドロップダウン リスト	サーバ上の 1 つ以上の物理コアを無効にできます。次のいずれかになります。 • [すべて（All）] : すべての物理コアを有効にします。 これにより、関連付けられている論理プロセッサ コアで Hyper Threading も有効になります。 • [1] ～ [28] : サーバで実行可能な論理プロセッサ コアの数を指定します。各物理コアには、論理コアが関連付けられています。 （注） オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせください。

[名前（Name）]	説明
[サブ NUMA クラスタリング（Sub NUMA Clustering）] ドロップダウンリスト	CPU がサブ NUMA クラスタリングをサポートするかどうか。そのクラスタリングでは、タグディレクトリとメモリ チャネルは常に同じ領域にあります。次のいずれかになります。 • [無効（disabled）][無効（Disabled）]：サブNUMAクラスタリングは発生しません。 • [有効（enabled）][有効（Enabled）]：サブ NUMA クラスタリングが発生します。 • [自動（Auto）][自動（auto）]：BIOS かサブNUMA のクラスタ リングされるかが決まります。
[IMC インターリーブ（IMC Interleave）] ドロップダウン リスト	この BIOS オプションは、Integrated Memory Controller（IMC）間のインターリーブを制御します。 • [一方向インターリーブ（1-way Interleave）]：インターリーブはありません。 • [双方向インターリーブ（2-way Interleave）]：2 つの IMC 間でアドレスがインターリーブされます。 • [自動（Auto）]：CPU が IMC のインターリーブ モードを決定します。
[XPT プリフェッチ（XPT Prefetch）] ドロップダウン リスト	XPTプリフェッチを使用して、最後のレベルのキャッシュに読み取り要求を送信できるようにして、その要求のコピーをメモリ コントローラのプリフェッチャに発行するかどうか。次のいずれかになります。 • [無効（disabled）][無効（Disabled）]：CPU は [XPT プリフェッチ（XPT Prefetch）] オプションを使用しません。 • [有効（enabled）][有効（Enabled）]：CPU は [XPT プリフェッチャ（XPT prefetcher）] オプションを有効にします。

[名前（Name）]	説明
[UPI プリフェッチ（UPI Prefetch）] ドロップダウン リスト	UPI プリフェッチは、DDR バス上でメモリ読み込みが早期に開始されるようにするメカニズムです。これは次のいずれかになります。 • [無効（disabled）][無効（Disabled）]：プロセッサでキャッシュデータをプリロードしません。 • [有効（enabled）][有効（Enabled）]：UPI プリフェッチャで最も関連性が高いと判断されたデータを含む L1 キャッシュをプリロードします。
[エネルギー パフォーマンスの BIOS 構成（Energy Performance BIOS Config）] ドロップダウン リスト	システムパフォーマンスまたはエネルギー効率がこのサーバで重要かどうかを判断できます。次のいずれかになります。 • [パフォーマンス（Performance）]：サーバでは、すべてのサーバ コンポーネントに全電力を常時提供します。このオプションでは、最高レベルのパフォーマンスが維持され、最大量の電力が必要となります。 • [バランス パフォーマンス（Balanced Performance）]：サーバは、すべてのサーバ コンポーネントに、パフォーマンスと電力のバランスを保つのに十分な電力を提供します。 • [バランス電力（Balanced Power）]：サーバは、すべてのサーバコンポーネントに、パフォーマンスと電力のバランスを保つのに十分な電力を提供します。 • [電力（Power）]：サーバは、すべてのサーバ コンポーネントに、消費電力の低減を維持するのに最大の電力を提供します。

[名前（Name）]	説明
[電力パフォーマンスの調整（Power Performance Tuning）] ドロップダウン リスト	BIOS または OS によってエネルギー パフォーマンスのバイアス調整をオンにできるかどうかを指定します。オプションは [BIOS] と [OS] です。 • [bios][BIOS]： エネルギー効率を調整する場合は [BIOS] を選択します。 • [os][OS]： エネルギー効率を調整する場合は [OS] を選択します。
[LLC プリフェッチ（LLC Prefetch）] ドロップダウン リスト	プロセッサが LLC プリフェッチ メカニズムを使用して日付をLLCにフェッチするかどうか。次のいずれかになります。 • [disabled][無効（Disabled）]：プロセッサでキャッシュデータをプリロードしません。 • [有効（enabled）][有効（Enabled）]：LLC プリフェッチャで最も関連性が高いと判断されたデータを含む L1 キャッシュをプリロードします。

[名前（Name）]	説明
[パッケージの C ステート（Package C State）]	アイドル時にサーバコンポーネントが使用できる電力量。次のいずれかになります。 • [no-limit][制限なし（No Limit）]：サーバは、使用可能な任意のCステートに入ることがあります。 • [自動（auto）][自動（Auto）]：物理的な高度をCPU が決定します。 • [C0 C1 ステート（C0 C1 State）]：サーバはすべてのサーバ コンポーネントに常にフル パワーを提供します。このオプションでは、最高レベルのパフォーマンスが維持され、最大量の電力が必要となります。 • [C2]：CPUのアイドル時に、システムの電力消費を C1 オプションよりもさらに低減します。この場合、必要な電力は C1 または C0 よりも少なくなりますが、サーバがハイ パフォーマンス モードに戻るのに要する時間が少し長くなります。 • [C6 保持なし（C6 Non Retention）]：CPU のアイドル時に、C3 オプションよりもさらに電力消費が低減されます。このオプションを使用すると、C0、C1、または C3 よりも電力量が節約されますが、サーバがフルパワーに戻るまでにパフォーマンス上の問題が発生する可能性があります。 • [C6 保持（C6 Retention）]：CPU のアイドル時に、C3 オプションよりもさらに電力消費が低減されます。このオプションを使用すると、C0、C1、または C3 よりも電力量が節約されますが、サーバがフルパワーに戻るまでにパフォーマンス上の問題が発生する可能性があります。

[名前（Name）]	説明
[ハードウェア P ステート（Hardware P-States）] ドロップダウン リスト	プロセッサハードウェアのPステートを有効にします。次のいずれかになります。 • [無効（disabled）][無効（Disabled）]：HWPMが無効になります。 • [hwpm-native-mode][HWPM ネイティブ モード（HWPM Native Mode）]：HWPMネイティブ モードがイネーブルになります。 • [hwpm-oob-mode][HWPM OOB モード（HWPM OOB Mode）]：HWPMアウトオブボックス モードがイネーブルになります。 • [レガシーなしのネイティブ モード（Native Mode with no Legacy）]（GUI のみ）

表 *5*：*[メモリ（Memory）]タブの BIOS パラメータ*

名称	説明
[ホストを即座にリブート（Reboot Host Immediately）] チェックボックス	オンにすると、ホストサーバが直ちに再起動されます。このチェックボックスは、変更を保存してからオンにする必要があります。
[NUMA] ドロップダウン リスト	BIOS で Non-Uniform Memory Access（NUMA）がサポートされているかどうか。次のいずれかになります。 • [無効（Disabled）]：サポートはディセーブルになっています。 • [有効（Enabled）]：サポートはイネーブルになっています。

名称	説明
[メモリ RAS 構成の選択（Select Memory RAS configuration）] ドロップダウン リスト	サーバに対するメモリの信頼性、可用性、およびサービス性（RAS）の設定方法。次のいずれかになります。 • [最大パフォーマンス（Maximum Performance）]：システムのパフォーマンスが最適化されます。 • [ミラー モード 1LM（Mirror Mode 1LM）]：システムのメモリの半分をバックアップとして使用することにより、システムの信頼性が最適化されます。
[4 G 以上の復号化（Above 4G Decoding）] ドロップダウン リスト	4 GB 以上の MMIO を有効または無効にします。次のいずれかになります。 • [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。 （注） 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ります。

表 *6*：*[電力/パフォーマンス（Power/Performance）] タブの BIOS パラメータ*

[名前（Name）]	説明
[ホストを即座にリブート（Reboot Host Immediately）] チェックボックス	オンにすると、ホスト サーバが直ちに再起動されます。このチェックボックスは、変更を保存してからオンにする必要があります。

[名前（Name）]	説明
[ハードウェア プリフェッチャ（Hardware Prefetcher）] ドロップダウン リスト	プロセッサで、インテル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、統合2次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。 • [無効（Disabled）]：ハードウェア プリフェッチャは使用しません。 • [有効（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。
[隣接キャッシュ ライン プリフェッチャ（Adjacent Cache Line Prefetcher）] ドロップダウン リスト	プロセッサで必要な行のみを取得するのではなく、偶数または奇数のペアのキャッシュ行を取得するかどうか。次のいずれかになります。 • [無効（Disabled）]：プロセッサで必要な行のみを取得します。 • [有効（Enabled）]：プロセッサで必要な行およびペアの行の両方を取得します。
[DCU ストリーマ プリフェッチ（DCU Streamer Prefetch）] ドロップダウン リスト	プロセッサで DCU IP Prefetch メカニズムを使用して履歴キャッシュ アクセス パターンを分析し、L1 キャッシュ内で最も関連性の高い行をプリロードします。次のいずれかになります。 • [無効（Disabled）]：プロセッサはキャッシュ読み取り要求を予測しようとせず、明示的に要求された行のみを取得します。 • [有効（Enabled）]：DCU Prefetcher でキャッシュ読み取りパターンを分析し、必要と判断した場合にキャッシュ内の次の行を事前に取得します。
[DCU IP プリフェッチャ（DCU IP Prefetcher）] ドロップダウン リスト	プロセッサで DCU IP Prefetch メカニズムを使用して履歴キャッシュ アクセス パターンを分析し、L1 キャッシュ内で最も関連性の高い行をプリロードします。次のいずれかになります。 • [無効（Disabled）]：プロセッサでキャッシュ データをプリロードしません。 • [有効（Enabled）]：DCU IP Prefetcher で最も関連性が高いと判断されたデータを含む L1 キャッシュをプリロードします。

[名前（Name）]	説明
[CPU パフォーマンス（CPU Performance）] ドロップダウンリスト	上記のオプションに対し CPU パフォーマンス プロファイルを設定します。次のいずれかになります。 • [エンタープライズ（Enterprise）]：すべてのオプションが有効です。 • [HPC]：すべてのオプションが有効です。 この設定はハイパフォーマンス コンピューティングとも呼ばれます。 • [高スループット（Hight Throughput）]：DCU IP プリフェッチャのみが有効になります。残りのオプションは無効になります。 • [カスタム（Custom）]：パフォーマンス プロファイルのすべてのオプションをサーバの BIOS セットアップから設定できます。また、[ハードウェア プリフェッチャ（Hardware Prefetcher）] オプションと [隣接キャッシュ ライン プリフェッチャ（Adjacent Cache Line Prefetcher）] オプションも同様に設定できます。

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 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と、正しい組み合わせのトークン値で事前設定されたトークン ファイルを使用できます。使用可能な事前設定されたプロファイルには、仮想化、高性能、低電力などがあります。シスコの Web サイトからこれらの事前設定されたトークン ファイルのさまざまなオプションをダウンロードして、BMC を使用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て、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、応答時間を待機する必要なく、プロファイルを自分の要件に合うように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 サーバの場所から、またはブラウザのクライアントを介して BIOS プロファイルをアップロードできます。

はじめる前に

このタスクを実行するには、admin 権限で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 作業ウィンドウの [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（Name）]	説明
[BIOS プロファイルのアップロード元（Upload BIOS Profile from）] ドロップダウン リスト	リモート サーバのタイプ。次のいずれかになります。 • TFTP • FTP • SFTP • SCP • HTTP
[サーバ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の IP アドレスまたはホスト名。[BIOS プロファイルのアップロード元（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。
[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。

[名前（Name）]	説明
[アップロード（Upload）] ボタン	選択された 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しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「サーバ（*RSA*）キー 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?*）」というメッセージとともにポップアップ ウィンドウが表示されます。サーバ フィンガープリントの信頼性に応じて、[はい（Yes）] または [いいえ（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に基づいており、接続先のホストを識別または確認できます。
[キャンセル（Cancel）] ボタン	サーバに保存されたファームウェア バージョンを変更せずにウィザードを終了します。

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 プロファイル）] 領域の [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（Name）]	説明
[ファイル（File）] フィールド	アップロードする BIOS プロファイル。
[参照（Browse）] ボタン	該当するファイルに移動するためのダイアログボックスが開きます。

次の作業

BIOS プロファイルをアクティブにします。

BIOS プロファイルの有効化

はじめる前に

このタスクを実行するには、admin 権限で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 作業ウィンドウの [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）] をクリックして、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

はじめる前に

このタスクを実行するには、admin 権限で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 作業ウィンドウの [BIOS] 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、[削除（Delete）] をクリックします。

ステップ 5 プロンプトで、[OK] をクリックして、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

はじめる前に

このタスクを実行するには、admin 権限で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 作業ウィンドウの [BIOS] 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、[バックアップを取得（Take Backup）] をクリックします。

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

次の作業

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

はじめる前に

このタスクを実行するには、admin 権限で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 作業ウィンドウの [BIOS] 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、[詳細（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（Name）]	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指定された値が表示されます。

[名前（Name）]	説明
[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。

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 [変更の保存（Save Changes）] をクリックします。

第 5 章

サーバのプロパティの表示

この章の内容は、次のとおりです。

CPU のプロパティの表示

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 [インベントリ（Inventory）] をクリックします。

ステップ 3 [インベントリ（Inventory）] ペインの [CPU] タブをクリックします。

ステップ 4 各 CPU の次の情報を確認します。

[名前（Name）]	説明
[ソケット名（Socket Name）] フィールド	CPU が装着されているソケット。
[ベンダー（Vendor）] フィールド	CPU のベンダー。

[名前（Name）]	説明
[ステータス（Status）] フィールド	CPU のステータス。
[ファミリ（Family）] フィールド	この CPU が属するファミリ。
[速度（Speed）] フィールド	CPU の速度（メガヘルツ単位）。
[コア数（Number of Cores）] フィールド	CPU のコアの数。
[署名（Signature）] フィールド	CPU の署名情報。
[スレッド数（Number of Threads）] フィールド	CPU が同時に処理できる最大スレッド数

メモリのプロパティの表示

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 [インベントリ（Inventory）] をクリックします。

ステップ 3 [インベントリ（Inventory）] ペインの [メモリ（Memory）] タブをクリックします。

ステップ 4 [メモリ サマリー（Memory Summary）] 領域で、メモリに関する次のサマリー情報を確認します。

名称	説明
[メモリ速度（Memory Speed）] フィールド	メモリ速度（メガヘルツ単位）。
[障害メモリ（Failed Memory）] フィールド	現在障害が発生しているメモリの量（メガバイト単位）。
[総メモリ（Total Memory）] フィールド	すべての DIMM が完全に機能している場合に、サーバで使用できるメモリの合計量。
[無視されるメモリ（Ignored Memory）] フィールド	現在使用できないメモリの量（メガバイト単位）。

名称	説明
[有効なメモリ（Effective Memory）] フィールド	現在サーバが使用できる実際のメモリの量。
[無視される DIMM の数（Number of Ignored DIMMs）] フィールド	サーバがアクセスできない DIMM の数。
[冗長メモリ（Redundant Memory）] フィールド	冗長ストレージに使用されるメモリの量。
[障害が発生した DIMM の数（Number of Failed DIMMs）] フィールド	障害が発生し、使用できない DIMM の数。
[使用可能なメモリ RAS（Memory RAS Possible）] フィールド	サーバでサポートされている RAS メモリ構成の詳細。
[メモリの設定（Memory Configuration）] フィールド	現在のメモリ設定。次のいずれかになります。 • [最大パフォーマンス（Maximum Performance）]：システムは自動的にメモリのパフォーマンスを最適化します。 • [ミラーリング（Mirroring）]：サーバはメモリ内のデータのコピーを 2 つ保持します。このオプションを使用すると、サーバ上の使用可能なメモリが等分され、その半分はミラー コピー用に自動的に予約されます。 • [ロックステップ（Lockstep）]：サーバ内の DIMM ペアが、同一のタイプ、サイズ、および構成を持ち、SMI チャネルにまたがって装着されている場合、ロックステップ モードを有効にして、メモリ アクセス遅延の最小化およびパフォーマンスの向上を実現できます。
DIMM 配置図（DIMM location diagram）	現在のサーバの DIMM またはメモリのレイアウトを示します。

ステップ 5 [DIMM ブラック リスト（DIMM Black Listing）] 領域で、DIMM の全体のステータスを確認し、DIMM のブラックリスト化を有効にします。

名称	説明
[全体の DIMM ステータス（Overall DIMM Status）] フィールド	DIMM の全体的なステータス。次のいずれかになります。 • [良好（Good）]：DIMM ステータスは使用可能です。 • [深刻な障害（Severe Fault）]：修正不可能な ECC エラーがある場合の DIMM ステータス。
[DIMM のブラックリストのイネーブル化（Enable DIMM Black List）] チェックボックス	DIMM のブラックリスト化を有効にする場合はこのオプションをオンにします。

ステップ 6 [メモリの詳細（Memory Details）] テーブルで、各 DIMM に関する次の詳細情報を確認します。

ヒント カラムの見出しをクリックすると、そのカラムのエントリに従って表の行がソートされます。

名称	説明
[名前（Name）] カラム	メモリ モジュールが装着されている DIMM スロットの名前
[容量（Capacity）] カラム	DIMM のサイズ。
[チャネル速度（Channel Speed）] カラム	メモリ チャネルのクロック速度（メガヘルツ単位）。
[チャネルタイプ（Channel Type）] カラム	メモリ チャネルのタイプ。
[メモリタイプの詳細（Memory Type Detail）] カラム	デバイスで使用されるメモリのタイプ。
[バンク ロケータ（Bank Locator）] カラム	メモリ バンク内の DIMM の場所。

名称	説明
[製造元（Manufacturer）] カラム	製造業者のベンダー ID。次のいずれかになります。 • [0x2C00]：Micron Technology, Inc. • [0x5105]：Qimonda AG i. In. • [0x802C]：Micron Technology, Inc. • [0x80AD]：Hynix Semiconductor Inc. • [0x80CE]：Samsung Electronics, Inc. • [0x8551]：Qimonda AG i. In. • [0xAD00]：Hynix Semiconductor Inc. • [0xCE00]：Samsung Electronics, Inc.
[シリアル番号（Serial Number）] カラム	DIMM のシリアル番号。
[アセット タグ（Asset Tag）] カラム	DIMM に関連付けられたアセット タグ（存在する場合）。
[製品番号（Part Number）] カラム	ベンダーによって割り当てられた DIMM の製品番号。
[可視性（Visibility）] カラム	DIMM がサーバに対して使用可能であるかどうか。
[操作性（Operability）] カラム	DIMM が現在正常に動作しているかどうか。
[データ幅（Data Width）] カラム	DIMM がサポートするデータの量（ビット単位）。

PCI アダプタのプロパティの表示

はじめる前に

サーバの電源をオンにする必要があります。そうしないと、プロパティが表示されません。

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 [インベントリ（Inventory）] をクリックします。

ステップ 3 [インベントリ（Inventory）] ペインの [PCI アダプタ（PCI Adapters）] タブをクリックします。

ステップ 4 [PCI アダプタ（PCI Adapters）] 領域で、装着されている PCI アダプタに関する次の情報を確認します。

[名前（Name）]	**説明**
[スロットID（Slot ID）] カラム	アダプタが存在するスロット。
[製品名（Product Name）] 列	アダプタの名前。
[オプション ROM ステータス（Option ROM Status）] カラム	オプション ROM のステータスを示します。次のいずれかになります。 • [ロード済み（Loaded）]：カードでデータを使用できます。 • [未ロード（Unloaded）]：カードでデータを使用できません。 • [ロードエラー（Load Error）]：カードが存在し、オプション ROM が有効になっています。ただし、カードのエラーによりオプション ROM にロードできませんでした。
[ファームウェア バージョン（Firmware Version）] カラム	アダプタのファームウェア バージョン。 （注） 標準の UEFI インターフェイス経由でバージョンを提供するアダプタのファームウェア バージョンのみ表示されます。たとえば、Intel LOM や Emulex アダプタなどです。
[ベンダー ID（Vendor ID）] カラム	ベンダーによって割り当てられたアダプタ ID。
[サブ ベンダー ID（Sub Vendor ID）] カラム	ベンダーによって割り当てられているセカンダリ アダプタ ID。
[デバイス ID（Device ID）] カラム	ベンダーによって割り当てられたデバイス ID。
[サブ デバイス ID（Sub Device ID）] カラム	ベンダーによって割り当てられているセカンダリ デバイス ID。

ストレージのプロパティの表示

はじめる前に

サーバの電源をオンにする必要があります。そうしないと、プロパティが表示されません。

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 作業ウィンドウの [インベントリ（Inventory）] タブをクリックします。

ステップ 4 [ストレージ（Storage）] タブの [ストレージ（Storage）] 領域で、次の情報を確認します。

[名前（Name）]	説明
[コントローラ（Controller）] フィールド	コントローラ ドライブが存在する PCIe スロット。
[PCI スロット（PCI Slot）] フィールド	コントローラ ドライブが配置されている PCIe スロットの名前。
[製品名（Product Name）] フィールド	コントローラの名前。
[シリアル番号（Serial Number）] フィールド	ストレージ コントローラのシリアル番号。
[ファームウェア パッケージ ビルド（Firmware Package Build）] フィールド	アクティブなファームウェア パッケージのバージョン番号。
[製品ID（Product ID）] フィールド	コントローラの製品 ID。
[バッテリのステータス（Battery Status）] フィールド	バッテリのステータス。
[キャッシュ メモリ サイズ（Cache Memory Size）] フィールド	キャッシュ メモリのサイズ（MB 単位）。

[名前（Name）]	説明
[状況（Health）] フィールド	コントローラのヘルス状態。
[詳細（Details）] フィールド	コントローラの詳細へのリンク。

TPM のプロパティの表示

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 [インベントリ（Inventory）] をクリックします。

ステップ 3 [インベントリ（Inventory）] ペインの [TPM] タブをクリックします。

ステップ 4 次の情報を確認します。

[名前（Name）]	説明
[バージョン（Version）] カラム	TPM のバージョン。TPM のバージョン詳細情報が使用できない場合、このフィールドには [適用しない（NA）] と表示されます。
[プレゼンス（Presence）] カラム	ホスト サーバでの TPM モジュールの有無。 • [実装済み（Equipped）] : TPM はホスト サーバにあります。 • [空（Empty）] : TPM はホスト サーバにありません。
[モデル（Model）] カラム	TPM のモデル番号。TPM がホスト サーバにない場合、このフィールドには [適用しない（NA）] と表示されます。
[有効になっているステータス（Enabled Status）] カラム	TPM がイネーブルかどうか。 • [有効（Enabled）] : TPM はイネーブルです。 • [無効（Disabled）] : TPM はディセーブルです。 • [不明（Unknown）] : TPM はホスト サーバにありません。
[ベンダー（Vendor）] カラム	TPM ベンダーの名前。TPM がホスト サーバにない場合、このフィールドには [適用しない（NA）] と表示されます。

[名前（Name）]	説明
[アクティブ ステータス（Active Status）] カラム	TPM のアクティベーション ステータス。 • [アクティブ（Activated）]：TPM はアクティブです。 • [非アクティブ（Deactivated）]：TPM は非アクティブです。 • [不明（Unknown）]：TPM はホスト サーバにありません。 （注） TPM バージョン 2.0 をインストールしている一部の C シリーズ サーバでは、[アクティブ ステータス（Active Status）] は [適用しない（NA）] として表示されます。
[シリアル（Serial）] カラム	TPM のシリアル番号。TPM がホスト サーバにない場合、このフィールドには [適用しない（NA）] と表示されます。
[所有（Ownership）] カラム	TPM の所有ステータス。 • [所有済み（Owned）]：TPM は所有されています。 • [所有されていません（Unowned）]：TPM は所有されていません。 • [不明（Unknown）]：TPM はホスト サーバにありません。 （注） TPM バージョン 2.0 をインストールしている一部の C シリーズ サーバでは、[所有（Ownership）] ステータスは [適用しない（NA）] として表示されます。
[リビジョン（Revision）] カラム	TPM の改訂番号。TPM がホスト サーバにない場合、このフィールドには [適用しない（NA）] と表示されます。

PID カタログの表示

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）] タブをクリックします。

ステップ 2 [コンピューティング（Compute）] 作業領域で、[PID カタログ（PID Catalog）] タブをクリックします。

ステップ 3 [サマリー（Summary）] 領域で、PID カタログに関する次の概要情報を確認します。

[名前（Name）]	**説明**
[アップロード ステータス（Upload Status）] フィールド	PID カタログのダウンロード ステータス。これは次のいずれかになります。 • [ダウンロード中（Download in Progress）] • [ダウンロードに成功しました（Download Successful）] • [ダウンロード エラー：TFTP ファイルが見つかりません（Download Error - TFTP File Not Found）] • [ダウンロード エラー：接続に失敗しました（Download Error - Connection Failed）] • [ダウンロード エラー：アクセスが拒否されました（Download Error - Access Denied）] • [ダウンロード エラー：ファイルが見つかりません（Download Error - File Not Found）] • [ダウンロード エラー：ダウンロードが失敗しました（Download Error - Download Failed）] • [有効化に成功しました（Activation Successful）] • [エラー：不明（Error - Unknown）] • 該当なし
[アクティベーション ステータス（Activation Status）] フィールド	PID カタログのアクティベーション ステータス。
[現在アクティブなバージョン（Current Activated version）] フィールド	アクティブな PID カタログのバージョン。

ステップ 4 [CPU] テーブルで、CPU に関する次の情報を確認します。

[名前（Name）]	説明
[ソケット（Socket）] フィールド	CPU が装着されているソケット。
[製品ID（Product ID）] フィールド	CPU の製品 ID。
[モデル] フィールド	CPU のモデル番号。

ステップ 5 [メモリ（Memory）] テーブルで、メモリに関する次の情報を確認します。

[名前（Name）]	説明
[名前（Name）] フィールド	メモリ スロットの名前。
[製品ID（Product ID）] フィールド	ベンダーによって割り当てられたメモリ スロットの製品 ID。
[ベンダー ID（Vendor ID）] フィールド	ベンダーによって割り当てられた ID。
[容量（Capacity）] フィールド	メモリのサイズ。
[速度（MHz）（Speed (MHz)）] フィールド	メモリ速度（メガヘルツ単位）。

ステップ 6 [PCI アダプタ（PCI Adapters）] テーブルで、PCI アダプタに関する次の情報を確認します。

[名前（Name）]	説明
[スロット（Slot）] カラム	アダプタが存在するスロット。
[製品 ID（Product ID）] カラム	アダプタの製品 ID。
[ベンダー ID（Vendor ID）] カラム	ベンダーによって割り当てられたアダプタ ID。
[サブ ベンダー ID（Sub Vendor ID）] カラム	ベンダーによって割り当てられているセカンダリ アダプタ ID。
[デバイス ID（Device ID）] カラム	ベンダーによって割り当てられたデバイス ID。

[名前（Name）]	説明
[サブ デバイス ID（Sub Device ID）] カラム	ベンダーによって割り当てられているセカンダリ デバイス ID。

ステップ 7 [HDD] テーブルで、HDD に関する次の情報を確認します。

[名前（Name）]	説明
[ディスク（Disk）] フィールド	ハード ドライブのディスク。
[製品ID（Product ID）] フィールド	ハード ドライブの製品 ID。
[コントローラ（Controller）] フィールド	選択した Cisco Flexible Flash コントローラのシステム定義の名前。この名前は変更できません。
[ベンダー（Vendor）] フィールド	ハード ドライブのベンダー。
[モデル] フィールド	ハード ドライブのモデル。

第 6 章

センサーの表示

この章の内容は、次のとおりです。

シャーシ センサーの表示

電源センサーの表示

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）] 作業領域で、[電源（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（Name）]	説明
[冗長性ステータス（Redundancy Status）] フィールド	電源装置の冗長性のステータス。

[しきい値センサー（Threshold Sensors）] 領域

[名前（Name）]	説明
[センサー名（Sensor Name）] カラム	センサーの名前。

[名前（Name）]	説明
[センサー ステータス（Sensor Status）] カラム	センサーのステータス。次のいずれかになります。 • 不明 • [情報（Informational）] • 標準 • 警告 • クリティカル（Critical） • [回復不能（Non-Recoverable）]
[リーディング（Reading）] カラム	現在の電力使用量（ワット単位）。
[Critical 最小しきい値（Critical Threshold Min）] カラム	Critical の最小しきい値。
[Critical 最大しきい値（Critical Threshold Max）] カラム	Critical の最大しきい値。
[回復不可能な最小しきい値（Non-Recoverable Threshold Min）] カラム	回復不可能な最小しきい値。
[回復不可能な最大しきい値（Non-Recoverable Threshold Max）] カラム	回復不可能な最大しきい値。

[個別センサー（Discrete Sensors）] 領域

[名前（Name）]	説明
[センサー名（Sensor Name）] カラム	センサーの名前。

[名前（Name）]	説明
[センサー ステータス（Sensor Status）] カラム	センサーのステータス。次のいずれかになります。 • 不明 • [情報（Informational）] • 標準 • 警告 • クリティカル（Critical） • [回復不能（Non-Recoverable）]
[リーディング（Reading）] カラム	センサーの基本状態。

ファン センサーの表示

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）] 作業領域で、[ファン（Fan）] タブをクリックします。

ステップ 4 次のファン センサーのプロパティを確認します。

[名前（Name）]	説明
[センサー名（Sensor Name）] カラム	センサーの名前。

[名前（Name）]	説明
[センサー ステータス（Sensor Status）] カラム	センサーのステータス。次のいずれかになります。 • 不明 • [情報（Informational）] • 標準 • 警告 • クリティカル（Critical） • [回復不能（Non-Recoverable）]
[速度（RPMS）（Speed (RPMS)）] カラム	ファンの速度（RPM 単位）。
[Critical 最小しきい値（Critical Threshold Min）] カラム	Critical の最小しきい値。
[Critical 最大しきい値（Critical Threshold Max）] カラム	Critical の最大しきい値。
[回復不可能な最小しきい値（Non-Recoverable Threshold Min）] カラム	回復不可能な最小しきい値。
[回復不可能な最大しきい値（Non-Recoverable Threshold Max）] カラム	回復不可能な最大しきい値。

温度センサーの表示

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）] 作業領域で、[温度（Temperature）] タブをクリックします。

ステップ 4 次の温度センサーのプロパティを確認します。

[名前（Name）]	説明
[センサー名（Sensor Name）] カラム	センサーの名前。
[センサー ステータス（Sensor Status）] カラム	センサーのステータス。次のいずれかになります。 • 不明 • [情報（Informational）] • 標準 • 警告 • クリティカル（Critical） • [回復不能（Non-Recoverable）]
[気温（Temperature）] カラム	現在の温度（摂氏単位）。
[Critical 最小しきい値（Critical Threshold Min）] カラム	Critical の最小しきい値。
[Critical 最大しきい値（Critical Threshold Max）] カラム	Critical の最大しきい値。
[回復不可能な最小しきい値（Non-Recoverable Threshold Min）] カラム	回復不可能な最小しきい値。
[回復不可能な最大しきい値（Non-Recoverable Threshold Max）] カラム	回復不可能な最大しきい値。

電圧センサーの表示

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）] 作業領域で、[電圧（Voltage）] タブをクリックします。

ステップ 4 次の電圧センサーのプロパティを確認します。

[名前（Name）]	**説明**
[センサー名（Sensor Name）] カラム	センサーの名前。
[センサー ステータス（Sensor Status）] カラム	センサーのステータス。次のいずれかになります。 • 不明 • [情報（Informational）] • 標準 • 警告 • クリティカル（Critical） • [回復不能（Non-Recoverable）]
[電圧（V）（Voltage (V)）] カラム	現在の電圧（ボルト単位）。
[Critical 最小しきい値（Critical Threshold Min）] カラム	Critical の最小しきい値。
[Critical 最大しきい値（Critical Threshold Max）] カラム	Critical の最大しきい値。
[回復不可能な最小しきい値（Non-Recoverable Threshold Min）] カラム	回復不可能な最小しきい値。
[回復不可能な最大しきい値（Non-Recoverable Threshold Max）] カラム	回復不可能な最大しきい値。

電流センサーの表示

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）] 作業領域で、[電流（Current）] タブをクリックします。

ステップ 4 次の電流センサーのプロパティを確認します。

[名前（Name）]	**説明**
[センサー名（Sensor Name）] カラム	センサーの名前。
[センサー ステータス（Sensor Status）] カラム	センサーのステータス。次のいずれかになります。 • 不明 • [情報（Informational）] • 標準 • 警告 • クリティカル（Critical） • [回復不能（Non-Recoverable）]
[温度（C）（Temperature (C)）] カラム	現在の温度（摂氏単位）。
[Critical 最小しきい値（Critical Threshold Min）] カラム	Critical の最小しきい値。
[Critical 最大しきい値（Critical Threshold Max）] カラム	Critical の最大しきい値。
[回復不可能な最小しきい値（Non-Recoverable Threshold Min）] カラム	回復不可能な最小しきい値。
[回復不可能な最大しきい値（Non-Recoverable Threshold Max）] カラム	回復不可能な最大しきい値。

LED センサーの表示

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）] 作業領域で、[LED（LEDs）] タブをクリックします。

ステップ 4 次の LED センサーのプロパティを確認します。

[名前（Name）]	説明
[センサー名（Sensor Name）] カラム	センサーの名前。
[LED ステータス（LED Status）] カラム	LED が点灯、点滅、または消灯しているかどうか。
[LED の色（LED Color）] カラム	LED の現在の色。 色の意味の詳細については、使用しているサーバタイプに対応するハードウェアインストレーションガイドを参照してください。

ストレージ センサーの表示

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 [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 [ストレージ（Storage）] タブの [ストレージ センサー（Storage Sensors）] 領域で、サーバの次のストレージに関する統計情報を表示します。

[名前（Name）]	説明
[名前（Name）] カラム	ストレージ デバイスの名前。
[ステータス（Status）] カラム	ストレージ デバイスのステータスに関する簡単な説明。

第 7 章

リモート プレゼンスの管理

この章の内容は、次のとおりです。

Serial Over LAN の設定

Serial over LAN を使用すると、管理対象システムのシリアル ポートの入出力を IP 経由でリダイレクトできます。ホスト コンソールへ Cisco IMC を使用して到達する場合は、サーバで Serial over LAN を設定して使用します。

はじめる前に

Serial over LAN を設定するには、管理者権限のある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 作業ウィンドウの [リモート管理（Remote Management）] タブをクリックします。

ステップ 4 [リモート プレゼンス（Remote Presence）] ペインの [Serial over LAN] タブをクリックします。

ステップ 5 [Serial over LAN プロパティ（Serial over LAN Properties）] 領域で、次のプロパティを更新します。

[名前（Name）]	**説明**
[有効化（Enable）] チェックボックス	オンにすると、このサーバで Serial over LAN（SoL）がイネーブルになります。
[ボー レート（Baud Rate）] ドロップダウン リスト	システムが SoL 通信に使用するボー レート。次のいずれかになります。 • 9600 bps • 19.2 kbps • 38.4 kbps • 57.6 kbps • 115.2 kbps

[名前（Name）]	説明
[COM ポート（Com Port）] ドロップダウン リスト	システムが SoL 通信をルーティングするシリアル ポート。 （注） このフィールドは一部の C シリーズ サーバだけで使用できます。使用できない場合、サーバは、SoL 通信に COM ポート 0 を使用します。 次のいずれかを選択できます。 • [com0]：SoL 通信は、外部デバイスへの物理 RJ45 接続またはネットワーク デバイスへの仮想 SoL 接続をサポートする、外部からアクセス可能なシリアルポートである COM ポート 0 を介してルーティングされます。 このオプションを選択すると、システムは、SoL をイネーブルにし、RJ45 接続をディセーブルにします。これは、サーバが外部シリアルデバイスをサポートできなくなることを意味します。 • [com1]：SoL 通信は、SoL だけを介してアクセス可能な内部ポートである、COM ポート 1 経由でルーティングされます。 このオプションを選択した場合、COM ポート 1 上の SoL および COM ポート 0 上の物理 RJ45 接続を使用できます。 （注） COM ポート設定を変更すると、既存のすべての SoL セッションは切断されます。 （注） このオプションを使用できるのは一部の C シリーズ サーバだけです。
[SSH ポート（SSH Port）] フィールド	Serial over LAN に直接アクセスできるポート。このポートを使用すると、SoL へのダイレクト アクセスを提供する Cisco IMC シェルを迂回できます。 有効な範囲は 1024 ～ 65535 です。デフォルト値は 2400 です。 （注） SSH ポート設定を変更すると、既存のすべての SSH セッションは切断されます。

ステップ 6 [変更の保存（Save Changes）] をクリックします。

仮想メディアの設定

はじめる前に

仮想メディアを設定するには、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）] タブをクリックします。

ステップ 2 [コンピューティング（Compute）] タブの [リモート管理（Remote Management）] タブをクリックします。

ステップ 3 [リモート管理（Remote Management）] タブで、[仮想メディア（Virtual Media）] タブをクリックします。

ステップ 4 [仮想メディア プロパティ（Virtual Media Properties）] 領域で、次のプロパティを更新します。

[名前（Name）]	**説明**
[有効化（Enable）] チェックボックス	オンにすると、仮想メディアがイネーブルになります。 （注） このチェックボックスをオフにすると、すべての仮想メディア デバイスはホストから自動的に切断されます。
[アクティブなセッション（Active Sessions）] フィールド	現在実行されている仮想メディア セッションの数。
[仮想メディア暗号化の有効化（Enable Virtual Media Encryption）] チェックボックス	オンにすると、すべての仮想メディア通信は暗号化されます。
[低電力 USB を有効（Low Power USB enabled）] チェックボックス	これを選択すると、低電力 USB が有効になります。 低電力 USB が有効化された場合、ISO をマッピングしてホストを再起動した後、ブート選択メニューに仮想ドライブが表示されます。 ただし、UCS VIC P81E カードのあるサーバに ISO をマッピングするときに、NIC が Cisco Card モードである場合、仮想ドライブがブート選択メニューに表示されるようにするには、このオプションを無効にする必要があります。

ステップ 5 [変更の保存（Save Changes）] をクリックします。

Cisco IMC マップされた vMedia ボリュームの作成

はじめる前に

このタスクを実行するには、admin 権限で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 作業ウィンドウの [リモート管理（Remote Management）] タブをクリックします。

ステップ 4 [リモート管理（Remote Management）] タブで、[仮想メディア（Virtual Media）] タブをクリックします。

ステップ 5 [現在のマッピング（Current Mappings）] 領域で、[新しいマッピングの追加（Add New Mapping）] をクリックします。

ステップ 6 [新しいマッピングの追加（Add New Mapping）] 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（Name）]	説明
[ボリューム（Volume）] フィールド	マッピング用にマウントされるイメージの ID。
[マウント タイプ（Mount Type）] ドロップダウン リスト	The type of mapping.次のいずれかになります。 （注） 選択したマウント タイプの通信ポートがスイッチでイネーブルになっていることを確認します。たとえば、マウント タイプとして CIFS を使用している場合は、ポート 445（これはその通信ポートです）がスイッチでイネーブルになっていることを確認します。同様に、HTTP の場合はポート 80、HTTPS の場合は 443、NFS の場合は 2049 をそれぞれイネーブルにします。 • [NFS]：ネットワーク ファイル システム。 • [CIFS]：Common Internet File System。 • [WWW(HTTP/HTTPS)]：HTTP ベースまたは HTTPS ベースのシステム。 （注） 仮想メディアをマウントする前に、Cisco IMC はサーバに ping を実行することによって、エンドサーバへの到達可能性の確認を試みます。

[名前（Name）]	説明
[リモート共有（Remote Share）] フィールド	マップするイメージの URL。形式は選択された [マウント タイプ（Mount Type）] によって異なります。 • [NFS]：serverip:/share を使用します。 • [CIFS]：//serverip/share を使用します。 • [WWW(HTTP/HTTPS)]：http[s]://serverip/share を使用します。
[リモート ファイル（Remote File）] フィールド	リモート共有の .iso または .img ファイルの名前と場所。

[名前（Name）]	説明
[マウント オプション（Mount Options）] フィールド	

[名前（Name）]	説明
	カンマ区切りリストで入力される業界標準のマウント オプション。オプションは選択された [マウント タイプ（Mount Type）] によって異なります。 [NFS] を使用している場合は、このフィールドを空白のままにするか、次の中から 1 つ以上を入力します。 • ro • rw • nolock • noexec • soft • port=VALUE • timeo=VALUE • retry=VALUE [CIFS] を使用している場合は、このフィールドを空白のままにするか、次の中から 1 つ以上を入力します。 • soft • nounix • noserverino • guest • [username=VALUE]：guest が入力された場合は無視されます。 • [password=VALUE]：guest が入力された場合は無視されます。 • sec=VALUE リモート サーバとの通信時に認証に使用するプロトコル。CIFS 共有の設定に応じて、VALUE の値は次のいずれかになります。 ◦ [なし（None）]：認証は使用されません。 ◦ [Ntlm]：NT LAN Manager（NTLM）セキュリティ プロトコル。このオプションは、Windows 2008 R2 および Windows 2012 R2 でのみ使用します。 ◦ [Ntlmi]：NTLMi のセキュリティ プロトコル。このオプションは、CIFS Windows サーバでデジタル署名が有効な場合にのみ使用します。

[名前（Name）]	説明
	◦ [Ntlmssp]：NT LAN Manager のセキュリティ サポート プロバイダー（NTLMSSP）プロトコル。このオプションは、Windows 2008 R2 および Windows 2012 R2 でのみ使用します。 ◦ [Ntlmsspi]：NTLMSSPi プロトコル。このオプションは、CIFS Windows サーバでデジタル署名が有効な場合にのみ使用します。 ◦ [Ntlmv2]：NTLMv2 セキュリティ プロトコル。このオプションは、Samba Linux でのみ使用します。 ◦ [Ntlmv2i]：NTLMv2i のセキュリティ プロトコル。このオプションは、Samba Linux でのみ使用します。 [WWW(HTTP/HTTPS)] を使用している場合は、このフィールドを空白のままにするか、次を入力します。 • noauto （注） 仮想メディアをマウントする前に、Cisco IMC はサーバに ping を実行することによって、エンドサーバへの到達可能性の確認を試みます。 • username=VALUE • password=VALUE
[ユーザ名（User Name）] フィールド	指定した [マウント タイプ（Mount Type）] のユーザ名（必要な場合）。
[パスワード（Password）] フィールド	選択されたユーザ名のパスワード（必要な場合）。

ステップ 7 [保存（Save）] をクリックします。

Cisco IMC マップされた vMedia ボリューム プロパティの表示

はじめる前に

このタスクを実行するには、admin 権限で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 作業ウィンドウの [リモート管理（Remote Management）] タブをクリックします。

ステップ 4 [リモート管理（Remote Management）] タブで、[仮想メディア（Virtual Media）] タブをクリックします。

ステップ 5 [現在のマッピング（Current Mappings）] テーブルから行を選択します。

ステップ 6 [プロパティ（Properties）] をクリックし、次の情報を確認します。

[名前（Name）]	説明
[新しいマッピングの追加（Add New Mapping）] ボタン	新しいイメージを追加できるダイアログボックスが開きます。
[プロパティ（Properties）] ボタン	選択したイメージのプロパティを表示または変更できるダイアログボックスが開きます。
[マップ解除（Unmap）] ボタン	マウントされた vMedia のマップを解除します。
最後のマッピング ステータス（Last Mapping Status）	最後に試行されたマッピングのステータス。
[ボリューム（Volume）] カラム	イメージの ID。
[マウント タイプ（Mount Type）] ドロップダウン リスト	The type of mapping.
[リモート共有（Remote Share）] フィールド	イメージの URL。
[リモート ファイル（Remote File）] フィールド	イメージの厳密なファイル位置。
[ステータス（Status）] フィールド	マップの現在のステータス。次のいずれかになります。 • [OK]：マッピングは正常です。 • [進行中（In Progress）]：マッピングが進行中です。 • [古い（Stale）]：Cisco IMC にマッピングが古いという理由を示すテキスト文字列が表示されます。 • [エラー（Error）]：Cisco IMC にエラーの理由を示すテキスト文字列が表示されます。

Cisco IMC マップされた vMedia ボリュームの削除

はじめる前に

このタスクを実行するには、admin 権限で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 作業ウィンドウの [リモート管理（Remote Management）] タブをクリックします。

ステップ 4 [リモート管理（Remote Management）] タブで、[仮想メディア（Virtual Media）] タブをクリックします。

ステップ 5 [現在のマッピング（Current Mappings）] テーブルから行を選択します。

ステップ 6 [マップ解除（Unmap）] をクリックします。

既存の Cisco IMC vMedia イメージの再マッピング

はじめる前に

このタスクを実行するには、admin 権限で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 作業ウィンドウの [リモート管理（Remote Management）] タブをクリックします。

ステップ 4 [リモート管理（Remote Management）] タブで、[仮想メディア（Virtual Media）] タブをクリックします。

ステップ 5 [現在のマッピング（Current Mappings）] テーブルから行を選択します。

ステップ 6 [再マッピング（Remap）] をクリックします。

Cisco IMC vMedia イメージの削除

はじめる前に

このタスクを実行するには、admin 権限で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 作業ウィンドウの [リモート管理（Remote Management）] タブをクリックします。

ステップ 4 [リモート管理（Remote Management）] タブで、[仮想メディア（Virtual Media）] タブをクリックします。

ステップ 5 [現在のマッピング（Current Mappings）] テーブルから行を選択します。

ステップ 6 [削除（Delete）] をクリックします。

KVM コンソール

KVM コンソールは Cisco IMC からアクセス可能なインターフェイスであり、サーバへのキーボード、ビデオ、マウス（KVM）の直接接続をエミュレートします。KVM 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。

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、KVM 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

KVM 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。

（注） Windows Server 2003 の Internet Explorer 6 SP1 から KVM コンソールを起動すると、必要なファイルをダウンロードできないことがブラウザから報告されます。この場合、ブラウザの [Tools] メニューをクリックし、[Internet Options] を選択します。[Advanced] タブをクリックし、[Security] セクションの [Do not save encrypted pages to disk] チェックボックスをオフにします。KVM コンソールを再度起動します。

KVM コンソールの起動

KVM コンソールは、ホームページまたは [リモート管理（Remote Management）] 領域から起動できます。

手順

ステップ 1 ホームページからコンソールを起動するには、[ナビゲーション（Navigation）]ペインで、[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 [サマリー（Summary）] をクリックします。

ステップ 3 ツールバーから、[KVM の起動（Launch KVM）] をクリックし、[Java ベース KVM（Java based KVM）] または [HTML ベース KVM（HTML based KVM）] を選択します。

ステップ 4 または、[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 5 [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 6 作業ウィンドウの [リモート管理（Remote Management）] タブをクリックします。

ステップ 7 [リモート管理（Remote Management）] ペインで、[仮想 KVM（Virtual KVM）] タブをクリックします。

ステップ 8 [仮想 KVM（Virtual KVM）] タブで、[Java ベースの KVM コンソールの起動（Launch Java based KVM console）] または [HTML ベースの KVM コンソールの起動（Launch HTML based KVM console）] をクリックします。

ステップ 9 ポップアップ ウィンドウに表示された URL リンクをクリックし（HTML ベースの KVM コンソールのみ）、クライアント アプリケーションをロードします。KVM コンソールを起動するたびにリンクをクリックする必要があります。

仮想 KVM コンソール（HTML ベース）

KVM コンソールは Cisco IMC からアクセス可能なインターフェイスであり、サーバへのキーボード、ビデオ、マウス（KVM）の直接接続をエミュレートします。遠隔地のサーバから接続して制

御し、この KVM 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。

[ファイル（File）] メニュー

メニュー項目	説明
[ファイルにキャプチャ（Capture to File）] ボタン	JPG イメージとして現在の画面を保存できる [保存（Save）] ダイアログボックスが開きます。
[終了（Exit）] ボタン	KVM コンソールを閉じます。

[表示（View）] メニュー

メニュー項目	説明
[キーボード（Keyboard）]	ユーザがデータの入力に使用できるKVMコンソールの仮想キーボードを表示します。
更新（Refresh）	サーバの現在のビデオ出力を使用してコンソール表示を更新します。
[全画面（Full Screen）]	画面全体になるように KVM コンソールを拡大します。

[マクロ（Macros）] メニュー

リモート システムで実行するキーボード ショートカットを選択します。

メニュー項目	説明
[サーバ マクロ（Server Macros）] メニュー	Cisco IMC からダウンロードされたサーバ サイド マクロがある場合、表示します。サーバサイドマクロがダウンロードされていない場合、このメニュー項目は無効になります。
[静的マクロ（Static Macros）] メニュー	マクロの定義済みのセットを表示します。
[ユーザ定義マクロ（User Defined Macros）] メニュー	作成済みのユーザ定義マクロを表示します。
[管理（Manage）] ボタン	マクロの作成および管理ができる [ユーザ定義マクロの設定（Configure User Defined Macros）] ダイアログ ボックスを開きます。 システム定義されたマクロは削除できません。

[ツール（Tools）] メニュー

メニュー項目	説明

[セッション オプション（Session Options）]	以下の項目が指定できる [セッション オプション（Session Options）] ダイアログを開きます。
	• [スケーリング（Scaling）]：画面の縦横率を維持するかどうかを指定します。 [縦横比を維持（Maintain Aspect Ratio）] チェックボックスをオンまたはオフにします（デフォルトはオン）。
	• ターゲット システムで使用するマウス アクセラレーション。デフォルトは、[絶対配置（Windows、Newer Linux & MAC OS X）（Absolute positioning (Windows, Newer Linux & MAC OS X)）] です。その他のオプションを次に示します。
	  • [相対的な位置付け、アクセラレーションなし（Relative Positioning, no acceleration）]
	  • [相対的な位置付け（RHEL、古い Linux）（Relative Positioning (RHEL, Older Linux)）]

[セッション ユーザ リスト（Session User List）]	アクティブ KVM セッションを持つすべてのユーザ ID を表示する [セッション ユーザ リスト（Session User List）] ダイアログ ボックスを開きます。
チャット（Chat）	他のユーザと通信するための [チャット（Chat）] ボックスを開きます。

[電源（Power）] メニュー

メニュー項目	説明
[システムの電源オン（Power On System）] ボタン	システムの電源を入れます。 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。
[システムの電源オフ（Power Off System）] ボタン	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。 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。

メニュー項目	説明
[システムのリセット(ウォーム ブート)（Reset System (warm boot)）] ボタン	電源をオフにすることなくシステムを再起動します。 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。
[システムの電源の再投入(コールド ブート)（Power Cycle System (cold boot)）] ボタン	システムの電源をオフにしてから、再度オンにします。 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。

[ブート デバイス（Boot Device）] メニュー

[名前（Name）]	説明
[オーバーライドなし（No Override）]	このオプションをオンにすると、ホストは設定されている最初のデバイスを起動できます。
[ブート デバイス（Boot Device）] リスト	サーバの起動に使用するブートデバイスのリスト。次回のサーバ ブートに対してのみ使用され、現在設定されているブート順序が乱されることはありません。ワン タイム ブート デバイスからサーバを起動すると、以前設定されたブート順からすべての機能のリブートが発生します。最大 15 のデバイスが KVM コンソールに表示されます。

[仮想メディア（Virtual Media）] メニュー

[名前（Name）]	説明
[仮想デバイスの有効化（Activate Virtual Devices）]	vMedia セッションをアクティブにし、ユーザがローカル コンピュータまたはネットワークから、ドライブまたはイメージファイルをアタッチできるようにします。

[名前（Name）]	説明
イメージの作成（Create Image） （注） このオプションは、Google Chrome Web ブラウザを使用している場合にのみ利用できます。	ISO イメージを作成できます。[イメージの作成（Create Image）] ダイアログボックスにファイルまたはフォルダをドラッグアンドドロップします。それらのファイルやフォルダは ISO イメージに変換されます。[ISO イメージのダウンロード（Download ISO Image）] ボタンを使用すると、ISO イメージをローカルマシンに保存できます。
[CD/DVD のマップ（Map CD/DVD）]	ローカル マシンから CD または DVD イメージをマップし、イメージにドライブをマップできます。 （注） このオプションは、[仮想デバイスのアクティブ化（Activate Virtual Devices）] をクリックすると使用可能になります。
[削除可能ディスクのマップ（Map Removable Disk）]	ローカル マシンから削除可能ディスク イメージをマップし、イメージにドライブをマップできます。 （注） このオプションは、[仮想デバイスのアクティブ化（Activate Virtual Devices）] をクリックすると使用可能になります。
[フロッピー ディスクのマップ（Map Floppy Disk）]	ローカルマシンからフロッピーディスクイメージをマップし、イメージにドライブをマップできます。 （注） このオプションは、[仮想デバイスのアクティブ化（Activate Virtual Devices）] をクリックすると使用可能になります。

[ヘルプ（Help）] メニュー

[名前（Name）]	説明
ヘルプ トピック（Help Topics）	このオプションをクリックすると、このウィンドウに戻ります。
[KVM ビューアについて（About KVM Viewer）]	KVM ビューアのバージョン番号を表示します。

設定

[設定（Settings）] アイコンは、HTML KVM ビューア ウィンドウの右上隅にあります。

[名前（Name）]	説明
[次のユーザとしてログイン:（Logged in as:）]	ユーザ ロール ID を表示します。
ホスト名（Host Name）	ホスト名を表示します。
ログアウト	KVM ビューアからログアウトできます。

Java ベース KVM と HTML5 ベース KVM の比較

次の表に、Java ベース KVM と HTML5 ベース KVM の間の相違点を示します。

メニュー オプション	操作	Java ベース KVM で使用可能	HTML5 ベース KVM で使用可能
ファイル（File）	オープン（Open）	○	○
	ファイルにキャプチャ（Capture to file）	○	○
	クリップボードからテキストの貼り付け（Paste Text from Clipboard）	[はい（Yes）]	[いいえ（No）]
	ファイルからテキストの貼り付け（Paste Text from File）	[はい（Yes）]	[いいえ（No）]
	Exit	○	○
表示（View）	更新（Refresh）	○	○
	自動調整（Fit）	[はい（Yes）]	[いいえ（No）]
	ビデオの拡大縮小（Video-Scaling）	[はい（Yes）]	[いいえ（No）]
	全画面（Full-Screen）	○	○
	Mini-Mod	[はい（Yes）]	[いいえ（No）]

メニュー オプション	操作	Java ベース KVM で使用可能	HTML5 ベース KVM で使用可能
マクロ（Macros）	サーバ マクロ（Server Macros）	○	○
	静的マクロ（Static Macros）	○	○
	ユーザ定義マクロ（User Defined Macros）	○	○
	管理	○	○
ツール	セッション オプション（Session Option）	○	○
	シングル カーソル（Single Cursor）	[はい（Yes）]	[いいえ（No）]
	Stats	[はい（Yes）]	[いいえ（No）]
	セッション ユーザ リスト（Session User List）	○	○
	チャット（Chat）	○	○
	レコーダー/再生コントロール（Recorder/Playback Controls）	[はい（Yes）]	[いいえ（No）]
	ビデオのエクスポート（Export Video）	[はい（Yes）]	[いいえ（No）]
電源（Power）	電源オン（Power On）	○	○
	電源オフ（Power OFF）	○	○
	システムのリセット（Reset System）	○	○
	電源の再投入システム（Power Cycle system）	○	○

メニュー オプション	操作	Java ベース KVM で使用可能	HTML5 ベース KVM で使用可能
	Mini-Mod	○	○
仮想メディア（Virtual Media）	イメージの作成（Create Image）	[はい（Yes）]	[いいえ（No）]
	仮想デバイスの有効化（Activate Virtual Devices）	○	○
	物理デバイス マッピング（Physical Device Mapping）	[はい（Yes）]	[いいえ（No）]

仮想 KVM の設定

はじめる前に

仮想 KVM 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 [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 作業ウィンドウの [リモート管理（Remote Management）] タブをクリックします。

ステップ 4 [リモート管理（Remote Management）] ペインで、[仮想 KVM（Virtual KVM）] タブをクリックします。

ステップ 5 で、次のフィールドに入力します。

[名前（Name）]	説明
[有効化（Enable）] チェックボックス	オンにすると、仮想 KVM がイネーブルになります。 （注） 仮想メディア ビューアにはKVMを使用してアクセスします。KVM コンソールをディセーブルにすると、Cisco IMC はホストに接続されているすべての仮想メディア デバイスへのアクセスもディセーブルにします。

[名前（Name）]	説明
[最大セッション数（Max Sessions）] ドロップダウン リスト	許可されている KVM の同時セッションの最大数。選択できる数値は 1 ～ 4 です。
[アクティブなセッション（Active Sessions）] フィールド	サーバで実行されている KVM セッションの数。
[リモート ポート（Remote Port）] フィールド	KVM 通信に使用するポート。
[ビデオ暗号化の有効化（Enable Video Encryption）] チェックボックス	オンにすると、サーバは KVM で送信されるすべてのビデオ情報を暗号化します。
[サーバのローカル ビデオの有効化（Enable Local Server Video）] チェックボックス	オンにすると、KVM セッションはサーバに接続されているすべてのモニタにも表示されます。

ステップ 6 [変更の保存（Save Changes）] をクリックします。

仮想 KVM のイネーブル化

はじめる前に

仮想 KVM をイネーブルにするには、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 作業ウィンドウの [リモート管理（Remote Management）] タブをクリックします。

ステップ 4 [リモート管理（Remote Management）] ペインで、[仮想 KVM（Virtual KVM）] タブをクリックします。

ステップ 5 で、[有効化（Enable）] チェックボックス をオンにします。

ステップ 6 [変更の保存（Save Changes）] をクリックします。

仮想 KVM のディセーブル化

はじめる前に

仮想KVMをディセーブルにするには、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 作業ウィンドウの [リモート管理（Remote Management）] タブをクリックします。

ステップ 4 [リモート管理（Remote Management）] ペインで、[仮想 KVM（Virtual KVM）] タブをクリックします。

ステップ 5 で、[有効化（Enable）] チェックボックスをオフにします。

ステップ 6 [変更の保存（Save Changes）] をクリックします。

第 8 章

ユーザ アカウントの管理

この章の内容は、次のとおりです。

ローカル ユーザの設定

Cisco IMC では、強力なパスワード ポリシーが実装されるようになったため、サーバに最初にログインした際に、ガイドラインに従って強力なパスワードを設定するよう要求されます。[ローカル ユーザ（Local User）] タブには [強力なパスワードの無効化（Disable Strong Password）] ボタンが表示され、そのボタンを使用することで、強力なパスワード ポリシーを無効にし、ガイドラインを無視して希望するパスワードを設定することができます。強力なパスワードを無効にすると、[強力なパスワードの有効化（Enable Strong Password）] ボタンが表示されます。デフォルトでは、強力なパスワード ポリシーが有効になっています。

はじめる前に

ローカル ユーザ アカウントを設定または変更するには、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 [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [ユーザ管理（User Management）] をクリックします。

ステップ 3 [ユーザ管理（User Management）] ペインの [ローカル ユーザ管理（Local User Management）] タブをクリックします。

ステップ 4 ローカル ユーザ アカウントを設定または変更するには、[ローカル ユーザ管理（Local User Management）] ペインの行をクリックして、[ユーザの変更（Modify User）] をクリックします。

ステップ 5 [ユーザの詳細の変更（Modify User Details）] ダイアログボックスで、次のプロパティを更新します。

[名前（Name）]	**説明**
[ID] フィールド	ユーザの固有識別情報。
[有効化（Enable）] チェックボックス	オンにすると、ユーザは Cisco IMC でイネーブルになります。
[ユーザ名（Username）] フィールド	ユーザのユーザ名。 1 ～ 16 文字の範囲で入力します。
[ロール（Role）] フィールド	ユーザに割り当てられているロール。次のいずれかになります。 • [読み取り専用（read-only）]：このロールのユーザは情報を表示できますが、変更することはできません。 • [ユーザ（user）]：このロールのユーザは、次のタスクを実行できます。 ◦ すべての情報を表示する ◦ 電源のオン、電源再投入、電源のオフなどの電力制御オプションを管理する ◦ KVM コンソールと仮想メディアを起動する ◦ すべてのログをクリアする ◦ ロケータ LED を切り替える ◦ タイム ゾーンを設定する ◦ ping • [管理者（admin）]：このロールのユーザは、GUI、CLI、IPMI で可能なすべてのアクションを実行できます。

[名前（Name）]	説明
[パスワードの変更（Change Password）] チェックボックス	オンにすると、変更を保存した場合、このユーザのパスワードが変更されます。新しいユーザ名の場合は、このチェックボックスをオンにする必要があります。
[新しいパスワード（New Password）] フィールド	このユーザ名のパスワード。フィールドの横の[ヘルプ（Help）] アイコンの上にカーソルを重ねると、パスワードを設定する際の以下のガイドラインが表示されます。 • パスワードは 8 ～ 14 文字とすること。 • パスワードにユーザ名を含めないこと。 • パスワードには次の 4 つのカテゴリの中から 3 つに該当する文字を含めること。 ◦ 大文字の英字（A ～ Z）。 ◦ 小文字の英字（a ～ z）。 ◦ 10 進数の数字（0 ～ 9）。 ◦ アルファベット以外の文字（!、@、#、$、%、^、&、*、-、_、=、"）。 これらのルールは、セキュリティ上の理由からユーザ用の強力なパスワードを定義するためのものです。ただし、これらのガイドラインを無視して希望するパスワードを設定する場合は、[ローカルユーザ（Local Users）] タブで [強力なパスワードの無効化（Disable Strong Password）] ボタンをクリックします。強力なパスワード オプションが無効にされている場合は、1 ～ 20 文字のパスワードを設定できます。
[新しいパスワードの確認（Confirm New Password）] フィールド	確認のためのパスワードの再入力。

ステップ 6 パスワード情報を入力します。

ステップ 7 [変更の保存（Save Changes）] をクリックします。

パスワードの有効期限切れ

パスワードの有効期限を設定することができ、その期限を過ぎるとパスワードは期限切れになります。管理者として、この時間を日数で設定できます。この設定は、すべてのユーザに共通です。パスワードの期限が切れると、ユーザはログイン時に通知され、パスワードをリセットしない限りログインできなくなります。

（注） 古いデータベースにダウングレードした場合、既存のユーザが削除されます。データベースはデフォルト設定に戻ります。以前に設定されたユーザは消去され、データベースは空になります。つまり、データベースのユーザ名はデフォルトの「admin」、パスワードは「password」となります。サーバにはデフォルトのユーザ データベースが残っているため、デフォルトのクレデンシャルの変更機能が有効になっています。これは、ダウングレード後に「admin」ユーザがデータベースに初めてログインする際に、そのユーザはデフォルトのクレデンシャルを強制的に変更する必要があることを意味します。

パスワード設定時刻

「パスワード設定時刻」は、すべての既存ユーザに対し、移行またはアップグレードが発生した時刻に設定されています。新規ユーザ（アップグレード後に作成されたユーザ）の場合、パスワード設定時刻は、ユーザが作成され、パスワードが設定された時刻に設定されます。一般ユーザ（新規および既存）の場合、パスワード設定時刻は、パスワードが変更されるたびに更新されます。

パスワードの有効期間の設定

はじめる前に

- パスワードの有効期限を有効に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 [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [ユーザ管理（User Management）] をクリックします。

ステップ 3 [ローカル ユーザ管理（Local User Management）] ペイン（デフォルトで開きます）で、[パスワードの有効期限の詳細（Password Expiration Details）] をクリックします。

ステップ 4 [パスワードの有効期限の詳細（Password Expiration Details）] 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（Name）]	説明
[パスワードの有効期限の有効化（Enable Password Expiry）] 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、[パスワードの有効期間（Password Expiry Duration）] を設定できます。無効にするには、このチェックボックスをオフにします。

[名前（Name）]	説明
[パスワードの有効期間（Password Expiry Duration）] フィールド	既存のパスワードに設定できる有効期間（その時間以後、新しいパスワードを設定するか、または既存のパスワードを変更します。）範囲は 1 ～ 3650 日です。
[パスワード履歴（Password History）] フィールド	パスワードが入力された回数。これを有効にすると、パスワードを繰り返すことができません。0～5の間の値を入力します。0 を入力すると、このフィールドが無効になります。
[通知期間（Notification Period）] フィールド	パスワードの期限が切れる時間を通知します。0 ～ 15 日の間の値を入力します。0 を入力すると、このフィールドが無効になります。
[猶予期間（Grace Period）] フィールド	既存のパスワードをまだ使用できる期間。この期間の後、パスワードは期限切れになります。0～5日の間の値を入力します。0 を入力すると、このフィールドが無効になります。

ステップ 5 [変更の保存（Save Changes）] をクリックします。

ステップ 6 必要に応じて、[値のリセット（Reset Values）] をクリックして、テキスト フィールドをクリアし、入力した値をリセットします。デフォルト設定に戻すには、[デフォルトに戻す（Restore Defaults）] をクリックします。

パスワード有効期限の有効化

はじめる前に

手順

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

ステップ 2 [管理者（Admin）] メニューの [ユーザ管理（User Management）] をクリックします。

ステップ 3 [ローカル ユーザ管理（Local User Management）] ペイン（デフォルトで開きます）で、[パスワードの有効期限の詳細（Password Expiration Details）] をクリックします。

ステップ 4 [パスワードの有効期限の詳細（Password Expiration Details）] ダイアログ ボックスで、[パスワードの有効期限の有効化（Enable Password Expiry）] チェック ボックスをオンにします。
[パスワードの有効期間（Password Expiry Duration）] テキスト フィールドが編集可能になり、日数の数値を入力することで期間を設定できます。

次の作業

パスワードの有効期間を設定します。

LDAP サーバ

Cisco IMC では、情報をディレクトリ内で編成してこの情報へのアクセスを管理するディレクトリ サービスがサポートされます。Cisco IMC は、ネットワークでディレクトリ情報を保管および保守する Lightweight Directory Access Protocol（LDAP）をサポートします。さらに、Cisco IMC は Microsoft Active Directory（AD）もサポートします。Active Directory はさまざまなネットワーク サービスを提供するテクノロジーであり、LDAP と同様のディレクトリ サービス、Kerberos ベースの認証、DNS ベースの名前付けなどが含まれます。Cisco IMC は LDAP での Kerberos ベースの認証サービスを利用します。

Cisco IMC で LDAP が有効になっている場合、ローカル ユーザ データベース内に見つからない ユーザ アカウントに関するユーザ認証とロール許可は、LDAP サーバによって実行されます。LDAP ユーザ認証の形式は username@domain.com です。

[LDAP 設定（LDAP Settings）] 領域の [暗号化を有効にする（Enable Encryption）] チェックボックスをオンにすると、LDAP サーバへの送信データを暗号化するようサーバに要求できます。

LDAP サーバの設定

ユーザ認証および権限付与のために LDAP を使用するよう、Cisco IMC を設定できます。LDAP を使用するには、Cisco IMC に関するユーザ 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を設定します。Cisco IMC のユーザ ロールとロケールにマップされた既存の 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。

重要 スキーマの変更の詳細については、http://technet.microsoft.com/en-us/library/bb727064.aspx の記事を参照してください。

（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、Cisco IMC のユーザ 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できます。

LDAP サーバに対して次の手順を実行する必要があります。

手順

ステップ 1 LDAP 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 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（Properties）	値
Common Name	CiscoAVPair
LDAP Display Name	CiscoAVPair
Unique X500 Object ID	1.3.6.1.4.1.9.287247.1
説明	CiscoAVPair
構文	大文字小文字を区別した文字列

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

a) 左ペインで [クラス（Classes）] ノードを展開し、U を入力してユーザ クラスを選択します。
b) [属性（Attributes）] タブをクリックして、[追加（Add）] をクリックします。
c) C を入力して CiscoAVPair 属性を選択します。
d) [OK] をクリックします。

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

[役割（Role）]	CiscoAVPair 属性値
admin	shell:roles="admin"
user	shell:roles="user"
read-only	shell:roles="read-only"

（注） 属性に値を追加する方法の詳細については、http://technet.microsoft.com/en-us/library/bb727064.aspx の記事を参照してください。

次の作業

Cisco IMC を使用して LDAP サーバを設定します。

Cisco IMC での LDAP 設定およびグループ認証の設定

はじめる前に

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 [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [ユーザ管理（User Management）] をクリックします。

ステップ 3 [ユーザ管理（User Management）] ペインの [LDAP] をクリックします。

ステップ 4 [LDAP 設定（LDAP Settings）] 領域で、次のプロパティを更新します。

[名前（Name）]	説明
[LDAP の有効化（Enable LDAP）] チェックボックス	これを選択した場合、まず LDAP サーバによってユーザ認証とロール許可が実行された後、ローカルユーザデータベースに存在しないユーザ アカウントによって実行されます。
[ベース DN（Base DN）] フィールド	ベース識別名。このフィールドは、ユーザおよびグループのロード元を示します。 Active Directory サーバでは、これは dc=domain,dc=com という形式でなければなりません。
[ドメイン（Domain）] フィールド	すべてのユーザが属する必要のある IPv4 ドメイン。 グローバル カタログ サーバのアドレスを少なくとも 1 つ指定していない限り、このフィールドは必須です。
[暗号化を有効にする（Enable Encryption）] チェックボックス	これを選択した場合、サーバは LDAP サーバに送るすべての情報を暗号化します。
[CA 証明書のバインディングの有効化（Enable Binding CA Certificate）] チェックボックス	オンにすると、LDAP CA 証明書をバインドできます。
[タイムアウト（0 ～ 180）秒数（Timeout (0 - 180) seconds）]	LDAP 検索操作がタイムアウトするまで Cisco IMC が待機する秒数。 検索操作がタイムアウトになった場合、Cisco IMC はこのタブで次にリストされているサーバ（存在する場合）への接続を試行します。 （注） このフィールドに指定する値は、全体的な時間に影響を及ぼす可能性があります。

[名前（Name）]	説明
[ユーザ検索の優先順位（User Search Precedence）]	ローカル ユーザ データベースと LDAP ユーザ データベースの間の検索の順序を指定できます。次のいずれかになります。 • [ローカル ユーザ データベース（Local User Database）]（デフォルト設定） • [LDAP ユーザ データベース（LDAP User Database）]

（注） [暗号化を有効にする（Enable Encryption）] チェックボックスと [CA 証明書のバインディングの有効化（Enable Binding CA Certificate）] チェックボックスをオンにした場合は、[LDAP サーバ（LDAP Server）] フィールドに LDAP サーバの完全修飾ドメイン名（FQDN）を入力します。LDAP サーバの FQDN を解決するには、Cisco IMC ネットワークの優先 DNS を設定して適切な DNS IP アドレスを指定します。

ステップ 5 [LDAP サーバの設定（Configure LDAP Servers）] 領域で、次のプロパティを更新します。

[名前（Name）]	説明
[LDAP サーバの事前設定（Pre-Configure LDAP Servers）] オプション ボタン	これを選択すると、Active Directory は事前構成された LDAP サーバを使用します。
[LDAP サーバ（LDAP Servers）] フィールド	
サーバ	6 つの LDAP サーバの IP アドレス。 LDAP に Active Directory を使用している場合、サーバ 1、2、3 はドメイン コントローラで、サーバ 4、5、6 はグローバル カタログです。LDAP 用に Active Directory を使用していない場合は、最大で 6 つの LDAP サーバを構成できます。 （注） また、ホスト名の IP アドレスも提供できます。

[名前（Name）]	説明
[ポート（Port）]	サーバのポート番号。 LDAP に Active Directory を使用している場合、サーバ 1、2、3（ドメイン コントローラ）のデフォルト ポート番号は 389 です。サーバ 4、5、6（グローバル カタログ）のデフォルト ポート番号は 3268 です。 LDAPS 通信は TCP 636 ポートで発生します。グローバル カタログ サーバへの LDAPS 通信は TCP 3269 ポートで発生します。
[DNS を使用した LDAP サーバの設定（Use DNS to Configure LDAP Servers）] オプション ボタン	これを選択した場合、DNS を使って LDAP サーバへのアクセスを設定できます。
[DNS パラメータ（DNS Parameters）] フィールド	
ソース（Source）	DNS SRV 要求に使われるドメイン名を取得する方法を指定します。この属性の種類は次のとおりです。 • [抽出済み（Extracted）]：ログイン ID からのドメイン名抽出ドメインを使用するよう指定します。 • [設定済み（Configured）]：設定された検索ドメインの使用を指定します。 • [設定済み - 抽出済み（Configured-Extracted）]：設定された検索ドメインよりも、ログイン ID から抽出されるドメイン名を使用することを指定します。
検索するドメイン（Domain to Search）	DNS クエリーのソースとして機能する設定済みドメイン名。 ソースが [抽出済み（Extracted）] と指定される場合、このフィールドは無効になります。
検索するフォレスト（Forest to Search）	DNS クエリーのソースとして機能する設定済みフォレスト名。 ソースが [抽出済み（Extracted）] と指定される場合、このフィールドは無効になります。

ステップ 6 [バインディング パラメータ（Binding Parameters）] 領域で、次のプロパティを更新します。

[名前（Name）]	説明
方法	この属性の種類は次のとおりです。 • [匿名（Anonymous）]：ユーザ名とパスワードを NULL にする必要があります。このオプションが選択され、LDAP サーバで匿名ログインが設定されている場合は、ユーザがアクセスすることができます。 • [設定済みクレデンシャル（Configured Credentials）]：初期バインドプロセスに対して既知のクレデンシャル セットを指定する必要があります。初期バインド プロセスが成功した場合、ユーザ名の識別名（DN）が照会され、再バインディング プロセス用に再利用されます。再バインディング プロセスが失敗すると、ユーザはアクセスを拒否されます。 • [ログイン クレデンシャル（Login Credentials）]：ユーザ クレデンシャルが必要です。バインドプロセスが失敗すると、ユーザはアクセスを拒否されます。 デフォルトでは、[ログイン クレデンシャル（Login Credentials）] オプションが選択されます。
バインド DN（Binding DN）	ユーザの識別名（DN）。このフィールドは、バインディング方式として [設定済みクレデンシャル（Configured Credentials）] オプションを選択した場合にのみ編集可能になります。
[パスワード（Password）]	ユーザのパスワード。このフィールドは、バインディング方式として [設定済みクレデンシャル（Configured Credentials）] オプションを選択した場合にのみ編集可能になります。

ステップ 7 [検索パラメータ（Search Parameters）] 領域で、次のフィールドを更新します。

[名前（Name）]	説明
フィルタ属性（Filter Attribute）	このフィールドは、LDAP サーバ上のスキーマの設定済み属性に一致する必要があります。 デフォルトでは、このフィールドには [sAMAccountName] と表示されます。
グループ属性（Group Attribute）	このフィールドは、LDAP サーバ上のスキーマの設定済み属性に一致する必要があります。 デフォルトでは、このフィールドには [memberOf] と表示されます。
属性（Attribute）	ユーザのロールとロケール情報を保持するLDAP属性。このプロパティは、常に、名前と値のペアで指定されます。システムは、ユーザ レコードで、この属性名と一致する値を検索します。 LDAP 属性では、Cisco IMC ユーザ ロールおよびロケールにマップされる既存のLDAP属性を使用することも、スキーマを変更して新しい LDAP 属性を作成することもできます。（たとえば CiscoAvPair など）。 （注） このプロパティを指定しない場合、ユーザはログインできません。オブジェクトは LDAP サーバ上に存在していますが、このフィールドで指定される属性と正確に一致する必要があります。
階層化するグループ検索の深さ（1 ～ 128）（Nested Group Search Depth (1-128)）	LDAP グループ マップで別の定義済みグループ内にネストされたLDAPグループを検索するパラメータ。このパラメータは、ネストされたグループ検索の深さを定義します。

ステップ 8 （任意） [グループ認証（Group Authorization）] 領域で、次のプロパティを更新します。

[名前（Name）]	説明
[LDAP グループ認証（LDAP Group Authorization）] チェックボックス	これを選択した場合、ローカルユーザデータベースにないLDAPユーザに関しても、グループ レベルでユーザ認証が実行されます。 このチェックボックスをオンにすると、Cisco IMC は [グループの設定（Configure Group）] ボタンをイネーブルにします。

[名前（Name）]	説明
検索するグループのネスト レベル(1～128)（Nested Group Search Depth (1-128)）	LDAP グループ マップで別の定義済みグループ内にネストされた LDAP グループを検索するパラメータ。このパラメータは、ネストされたグループ検索の深さを定義します。
[グループ名（Group Name）] カラム	サーバへのアクセスが許可されているグループの名前を LDAP サーバ データベースに指定します。
[グループ ドメイン（Group Domain）] カラム	LDAP サーバのドメインがグループに存在する必要があります。
[ロール（Role）] カラム	すべてのユーザに割り当てられているこの LDAP サーバ グループのロール。次のいずれかになります。 • [読み取り専用（read-only）]：このロールのユーザは情報を表示できますが、変更することはできません。 • [ユーザ（user）]：このロールのユーザは、次のタスクを実行できます。 ◦ すべての情報を表示する ◦ 電源のオン、電源再投入、電源のオフなどの電力制御オプションを管理する ◦ KVM コンソールと仮想メディアを起動する ◦ すべてのログをクリアする ◦ ロケータ LED を切り替える ◦ タイム ゾーンを設定する ◦ ping • [管理者（admin）]：このロールのユーザは、GUI、CLI、IPMI で可能なすべてのアクションを実行できます。
[設定（Configure）] ボタン	Active Directory グループを設定します。
[削除（Delete）] ボタン	既存の LDAP グループを削除します。

ステップ 9 [変更の保存（Save Changes）] をクリックします。

ユーザ検索の優先順位の設定

はじめる前に

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 [管理者（Admin）] タブをクリックします。

ステップ 2 [管理者（Admin）] タブの [ユーザ管理（User Management）] をクリックします。

ステップ 3 [ユーザ管理（User Management）] ペインの [LDAP] タブをクリックします。

ステップ 4 [LDAP 設定（LDAP Settings）] 領域の [ユーザ検索の優先順位（User Search Precedence）] フィールドで、[ローカル ユーザ データベース（Local User Database）] または [LDAP ユーザ データベース（LDAP User Database）] を選択します。
このフィールドでは、上記のオプション間の検索順序を指定することができます。[ローカルユーザ データベース（Local User Database）] がデフォルトのオプションです。

次の作業

LDAP 証明書の概要

Cisco C シリーズ サーバでは、LDAP バインディング ステップ時に、LDAP クライアントがインストール済み CA 証明書またはチェーン CA 証明書に対してディレクトリ サーバ証明書を検証できるようになっています。リモート ユーザ認証のために信頼されたポイントまたはチェーン証明書を Cisco IMC に入力できないことにより、誰でもユーザ認証用のディレクトリ サーバを複製してセキュリティ違反が発生する恐れがある場合は、この機能を導入します。

暗号化された TLS/SSL 通信中にディレクトリ サーバ証明書を検証するには、LDAP クライアントに新しい設定オプションが必要です。

LDAP CA 証明書ステータスの表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理者（Admin）] タブをクリックします。

ステップ 2 [管理者（Admin）] メニューの [ユーザ管理（User Management）] をクリックします。

ステップ 3 [ユーザ管理（User Management）] ペインの [LDAP] タブをクリックします。

ステップ 4 [証明書ステータス（Certificate Status）] 領域で、次のフィールドの値を確認します。

[名前（Name）]	説明
ダウンロード ステータス	このフィールドには、LDAP CA 証明書のダウンロード ステータスが表示されます。
エクスポート ステータス（Export Status）	このフィールドには、LDAP CA 証明書のエクスポート ステータスが表示されます。

LDAP CA 証明書のエクスポート

はじめる前に

このアクションを実行するには、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。

署名付き LDAP CA 証明書をエクスポートするには、あらかじめ証明書がダウンロードされている必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理者（Admin）] タブをクリックします。

ステップ 2 [管理者（Admin）] メニューの [ユーザ管理（User Management）] をクリックします。

ステップ 3 [ユーザ管理（User Management）] ペインの [LDAP] タブをクリックします。

ステップ 4 [LDAP CA 証明書のエクスポート（Export LDAP CA Certificate）] リンクをクリックします。
[LDAP CA 証明書のエクスポート（Export LDAP CA Certificate）] ダイアログボックスが表示されます。

[名前（Name）]	説明
[リモートロケーションにエクスポート（Export to Remote Location）[	

[名前（Name）]	説明
	このオプションを選択することで、証明書をリモートの場所から選択してエクスポートできます。次の詳細を入力します。 • ◦ TFTP サーバ（TFTP Server） ◦ FTP サーバ（FTP Server） ◦ SFTP サーバ（SFTP Server） ◦ SCP サーバ ◦ HTTP サーバ（HTTP Server） （注） このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「サーバ（*RSA*）キー 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?*）」というメッセージとともにポップアップ ウィンドウが表示されます。サーバ フィンガープリントの信頼性に応じて、[はい（Yes）] または [いいえ（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に基づいており、接続先のホストを識別または確認できます。 • [サーバ IP/ホスト名（Server IP/Hostname）] フィールド：LDAP CA 証明書ファイルをエクスポートするサーバの IP アドレスまたはホスト名。[証明書のダウンロード元（Download Certificate from）] ドロップダウン リストの設定によって、このフィールドの名前は異なる場合があります。 • [パスおよびファイル名（Path and Filename）] フィールド：リモート サーバから証明書をダウンロードする際に Cisco IMC が使用するパスおよびファイル名。

[名前（Name）]	説明
	• [ユーザ名（Username）] フィールド：システムがリモート サーバにログインする際に使用するユーザ名。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。 • [パスワード（Password）] フィールド：リモート サーバのユーザ名に対応するパスワード。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。
[ローカルデスクトップにエクスポート（Export to Local Desktop）]	このオプションを選択することで、コンピュータのローカル ドライブに保管されている証明書を選択してエクスポートできます。

ステップ 5 [証明書のエクスポート（Export Certificate）] をクリックします。

LDAP CA 証明書のダウンロード

はじめる前に

- このアクションを実行するには、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。
- このアクションは、バインディング CA 証明書が有効にされていないと実行できません。

（注） Cisco IMC では CA 証明書またはチェーン CA 証明書のみを使用する必要があります。デフォルトの CA 証明書の形式は .cer です。チェーン CA 証明書を使用する場合は、Cisco IMC にダウンロードする前に .cer 形式に変換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 [管理者（Admin）] タブをクリックします。

ステップ 2 [管理者（Admin）] メニューの [ユーザ管理（User Management）] をクリックします。

ステップ 3 [ユーザ管理（User Management）] ペインの [LDAP] タブをクリックします。

ステップ 4 [LDAP CA 証明書のダウンロード（Download LDAP CA Certificate）] リンクをクリックします。
[LDAP CA 証明書のダウンロード（Download LDAP CA Certificate）] ダイアログボックスが表示されます。

[名前（Name）]	説明
[リモート ロケーションからダウンロード（Download from remote location）] オプション ボタン	このオプションを選択することで、証明書をリモートの場所から選択してダウンロードできます。次の詳細を入力します。 • ◦ TFTP サーバ（TFTP Server） ◦ FTP サーバ（FTP Server） ◦ SFTP サーバ（SFTP Server） ◦ SCP サーバ ◦ HTTP サーバ（HTTP Server） （注） このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「サーバ（*RSA*）キー 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?*）」というメッセージとともにポップアップ ウィンドウが表示されます。サーバ フィンガープリントの信頼性に応じて、[はい（Yes）] または [いいえ（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に基づいており、接続先のホストを識別または確認できます。 • [サーバ IP/ホスト名（Server IP/Hostname）] フィールド：LDAP CA 証明書ファイルを保管するサーバの IP アドレスまたはホスト名。[証明書のダウンロード元（Download Certificate from）] ドロップダウン リストの設定によって、このフィールドの名前は異なる場合があります。 • [パスおよびファイル名（Path and Filename）] フィールド：リモート サーバにファイルをダウンロードする際に Cisco IMC で使用するパスおよびファイル名。 • [ユーザ名（Username）] フィールド：システムがリモート サーバにログインする際に使用するユーザ名。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。 • [パスワード（Password）] フィールド：リモート サーバのユーザ名に対応するパスワード。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。

[名前（Name）]	説明
[ブラウザ クライアント経由でダウンロード（Download through browser client）] オプション ボタン	このオプションを選択することで、Cisco IMC GUI を実行しているコンピュータのローカル ドライブに保管されている証明書に移動できます。 このオプションを選択すると、Cisco IMC GUI に [参照（Browse）] ボタンが表示されます。このボタンを使用して、インポートするファイルに移動できます。
[証明書コンテンツの貼り付け（Paste Certificate content）] オプション ボタン	このオプションを選択することで、署名付き証明書の内容全体をコピーして [証明書コンテンツの貼り付け（Paste certificate content）] テキスト フィールドに貼り付けることができます。 （注） アップロードする前に証明書が署名済みであることを確認します。
[証明書のダウンロード（Download Certificate）] ボタン	証明書をサーバにダウンロードできます。

LDAP バインディングのテスト

はじめる前に

このアクションを実行するには、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。

（注） [暗号化を有効にする（Enable Encryption）] チェックボックスと [CA 証明書のバインディングの有効化（Enable Binding CA Certificate）] チェックボックスをオンにした場合は、[LDAP サーバ（LDAP Server）] フィールドに LDAP サーバの完全修飾ドメイン名（FQDN）を入力します。LDAP サーバの FQDN を解決するには、Cisco IMC ネットワークの優先 DNS を設定して適切な DNS IP アドレスを指定します。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理者（Admin）] タブをクリックします。

ステップ 2 [管理者（Admin）] メニューの [ユーザ管理（User Management）] をクリックします。

ステップ 3 [ユーザ管理（User Management）] ペインの [LDAP] タブをクリックします。

ステップ 4 [LDAP バインディングのテスト（Test LDAP Binding）] リンクをクリックします。

[LDAP CA 証明書のバインディングのテスト（Test LDAP CA Certificate Binding）] ダイアログボックスが表示されます。

[名前（Name）]	説明
[ユーザ名（Username）] フィールド	ユーザ名を入力します。
[パスワード（Password）] フィールド	対応するパスワードを入力します。

ステップ 5 [テスト（Test）] をクリックします。

LDAP CA 証明書の削除

はじめる前に

このアクションを実行するには、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 [管理者（Admin）] タブをクリックします。

ステップ 2 [管理者（Admin）] メニューの [ユーザ管理（User Management）] をクリックします。

ステップ 3 [ユーザ管理（User Management）] ペインの [LDAP] タブをクリックします。

ステップ 4 [LDAP CA 証明書の削除（Delete LDAP CA Certificate）] リンクをクリックし、[OK] をクリックして確定します。

ユーザ セッションの表示

手順

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

ステップ 2 [管理者（Admin）] メニューの [ユーザ管理（User Management）] をクリックします。

ステップ 3 [ユーザ管理（User Management）] ペインの [セッション管理（Session Management）] をクリックします。

ステップ 4 [セッション（Sessions）] ペインで、現在のユーザ セッションに関する次の情報を表示します。

[名前（Name）]	説明
[セッションの終了（Terminate Session）] ボタン	ユーザ アカウントに [管理者（admin）] ユーザ ロールが割り当てられている場合、このオプションを使用して、関連付けられているユーザ セッションを強制的に終了できます。 （注） このタブから現在のセッションを終了することはできません。
[セッション ID（Session ID）] カラム	セッションの固有識別情報。
[ユーザ名（User name）] カラム	ユーザのユーザ名。
[IP アドレス（IP Address）] カラム	ユーザがサーバにアクセスした IP アドレス。シリアル接続の場合は、[なし（N/A）] と表示されます。
[タイプ（Type）] カラム	ユーザがサーバにアクセスするために選択したセッション タイプ。次のいずれかになります。 • [webgui]：ユーザが Web UI を使用してサーバに接続されていることを示します。 • [CLI]：ユーザが CLI を使用してサーバに接続されていることを示します。 • [シリアル（serial）]：ユーザがシリアル ポートを使用してサーバに接続されていることを示します。
[アクション（Action）] カラム	このカラムには、SOL が有効の場合は [なし（N/A）] と表示され、SOL が無効の場合は [終了（Terminate）] と表示されます。Web UI で [終了（Terminate）] をクリックすることでセッションを終了できます。

第 9 章

シャーシ関連の設定

この章の内容は、次のとおりです。

サーバの電源管理

はじめる前に

このタスクを実行するには、user または admin 権限で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）] メニューの [サマリー（Summary）] をクリックします。

ステップ 3 作業ウィンドウ上部のツールバーで、[ホストの電源（Host Power）] リンクをクリックします。

ステップ 4 ドロップダウン リストから、次のいずれかのオプションを選択します。

アクション（Actions）	説明
[電源オン（Power ON）]	選択されたサーバの電源を投入します。

アクション（Actions）	説明
[電源オフ（Power Off）]	タスクがサーバで実行されていても、選択されたサーバの電源をオフにします。 **重要** ファームウェアまたはBIOSの更新が進行中の場合は、そのタスクが完了するまでサーバの電源をオフにしたり、サーバをリセットしたりしないでください。
[電源の再投入（Power Cycle）]	選択されたサーバの電源をオフ/オンにします。
[ハード リセット（Hard Reset）]	選択されたサーバをリブートします。
[シャットダウン（Shut Down）]	オペレーティングシステムがこの機能をサポートしている場合、選択されたサーバをシャットダウンします。

Web UI からのホスト名/IP アドレスへの Ping

はじめる前に

このタスクを実行するには、user または admin 権限でログインする必要があります。

手順

ステップ 1 作業ウィンドウ上部のツールバーで、[Ping] アイコンをクリックします。

ステップ 2 [Ping の詳細（Ping Details）] ダイアログボックスで、次のフィールドを更新します。

アクション（Actions）	説明
[*ホスト名/IP アドレス（*Hostname/IP Address）] フィールド	到達するホスト名または IP アドレス。
[*再試行回数（*Number of Retries）] フィールド	IP アドレスに ping を送ることが許可された再試行の最大数。デフォルト値は 3 です。値の範囲は 1 ～ 10 です。
[*タイムアウト（*Timeout）] フィールド	ping の最大応答時間。デフォルト値は 10 秒です。有効な範囲は 1 ～ 20 秒です。
[Ping ステータス（Ping Status）] フィールド	ping の結果を表示します。

アクション（Actions）	説明
[詳細（Details）] ボタン	ping アクティビティの詳細を表示します。
[Ping] ボタン	IP アドレスを ping します。
[キャンセル（Cancel）] ボタン	ping を実行せずにダイアログボックスを閉じます。

ステップ 3 [Ping] をクリックします。

ロケータ LED の切り替え

はじめる前に

このタスクを実行するには、user または admin 権限で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）] メニューの [サマリー（Summary）] をクリックします。

ステップ 3 作業ウィンドウ上部のツールバーで、[ロケータ LED（Locator LED）] リンクをクリックします。

ステップ 4 [ロケータ LED をオン（Turn On Locator LED）] または [ロケータ LED をオフ（Turn Off Locator LED）] を選択します。

タイム ゾーンの選択

はじめる前に

このタスクを実行するには、user または admin 権限で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）] メニューの [サマリー（Summary）] をクリックします。

ステップ 3 [Cisco Integrated Management Controller（Cisco IMC）の情報（Cisco Integrated Management Controller (Cisco IMC) Information）] 領域で、[タイムゾーンの選択（Select Timezone）] をクリックします。[タイムゾーンの選択（Select Timezone）] 画面が表示されます。

ステップ 4 [タイムゾーンの選択（Select Timezone）] ポップアップ画面で、マップの上にカーソルを移動してロケーションをクリックしてタイム ゾーンを選択するか、または [タイムゾーン（Timezone）] ドロップダウン メニューからタイム ゾーンを選択します。

ステップ 5 [保存（Save）] をクリックします。

第 10 章

ネットワーク関連の設定

この章の内容は、次のとおりです。

サーバ NIC の設定

サーバ NIC

NIC モード

NIC モード設定は、Cisco IMC に到達できるポートを決定します。プラットフォームに応じて、次のネットワーク モード オプションを使用できます。

- [専用（Dedicated）]：Cisco IMC へのアクセスに使用される管理ポート。
- [シスコ カード（Cisco Card）]：Cisco IMC にアクセスするために使用できるアダプタ カードの任意のポート。Cisco アダプタ カードは、ネットワーク通信サービス インターフェイス プロトコル サポート（NCSI）のあるスロットに取り付ける必要があります。

NIC 冗長化

選択した NIC モードとプラットフォームに応じて、次の NIC 冗長化オプションを使用できます。

- [アクティブ-アクティブ（active-active）] : サポートされている場合、設定されている NIC モードに関連付けられたすべてのポートが同時に動作します。この機能により、スループットが増加し、Cisco IMC への複数のパスが提供されます。
- [アクティブ-スタンバイ（active-standby）] : 設定されている NIC モードに関連付けられたポートで障害が発生した場合、トラフィックは、その NIC モードに関連付けられている他のポートの 1 つにフェールオーバーします。

（注） このオプションを選択する場合は、設定されている NIC モードに関連付けられたすべてのポートが同じサブネットに接続され、どのポートが使用されてもトラフィックの安全が保証されるようにする必要があります。

使用できる冗長化モードは、選択されているネットワーク モードとプラットフォームによって異なります。使用可能なモードについては、使用するサーバの『*Hardware Installation Guide*』（HIG）を参照してください。C シリーズの HIG は次の URL で入手できます。http://www.cisco.com/en/US/products/ps10493/prod_installation_guides_list.html

サーバ NIC の設定

NIC モードと NIC 冗長化を設定する場合は、サーバの NIC を設定します。

はじめる前に

NIC 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 [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [ネットワーキング（Networking）] をクリックします。

ステップ 3 [NIC プロパティ（NIC Properties）] 領域で、次のプロパティを更新します。

名称	説明Cisco IMC
[NIC モード（NIC Mode）] ドロップダウン リスト	Cisco IMC へのアクセスに使用できるポート。次のいずれかになります。 • [専用（Dedicated）]：Cisco IMC へのアクセスに使用される管理ポート。 • [シスコ カード（Cisco Card）]：Cisco IMC へのアクセスに使用できるアダプタ カード上の任意のポート。Cisco アダプタ カードは、ネットワーク通信サービス インターフェイス プロトコル サポート（NCSI）のあるスロットに取り付ける必要があります。
[VIC スロット（VIC Slot）] ドロップダウン リスト	Cisco カード モードで管理機能に使用できる VIC スロット。次のいずれかになります。 C220 M4 サーバでは、VIC スロット オプションは次のとおりです。 • [ライザー 1（Riser 1）]：スロット 1 が選択されます。 • [ライザー 2（Riser 2）]：スロット 2 が選択されます。 • [FLEX LOM]：スロット 3（MLOM）が選択されます。 C240 M4 サーバでは、VIC スロット オプションは次のとおりです。 • [ライザー 1（Riser 1）]：スロット 2 がプライマリ スロットですが、スロット 1 も使用できます。 • [ライザー 2（Riser 2）]：スロット 5 がプライマリ スロットですが、スロット 4 も使用できます。 • [FLEX LOM]：スロット 7（MLOM）が選択されます。 次のオプションを使用できるのは一部の UCS C シリーズ サーバだけです。 • 4 • 5 • [9] • 10 （注） このオプションを使用できるのは一部の UCS C シリーズ サーバだけです。

名称	説明Cisco IMC
[VIC スロット（VIC Slot）] ドロップダウン リスト	Cisco カード モードで管理機能に使用できる VIC スロット。次のいずれかになります。 C220 M5 サーバでは、VIC スロット オプションは次のとおりです。 • [ライザー 1（Riser 1）]：スロット 1 が選択されます。 • [ライザー 2（Riser 2）]：スロット 2 が選択されます。 • [FLEX LOM]：スロット 3（MLOM）が選択されます。 C240 M5 サーバでは、VIC スロット オプションは次のとおりです。 • [ライザー 1（Riser 1）]：スロット 2 がプライマリ スロットですが、スロット 1 も使用できます。 • [ライザー 2（Riser 2）]：スロット 5 がプライマリ スロットですが、スロット 4 も使用できます。 • [FLEX LOM]：スロット 7（MLOM）が選択されます。 次のオプションを使用できるのは一部の UCS C シリーズ サーバだけです。 • 4 • 5 • [9] • 10 （注） このオプションを使用できるのは一部の UCS C シリーズ サーバだけです。
[SIOC スロット（SIOC Slot）]	Cisco IMC ネットワーク モードを表示します。システム I/O コントローラ（SIOC1）にあるカードに基づいて、ネットワーク モードは 1 または 2 になります。 （注） このオプションを使用できるのは一部の UCS C シリーズ サーバだけです。

名称	説明Cisco IMC
[NIC 冗長化（NIC Redundancy）] ドロップダウンリスト	使用可能なNIC冗長オプションは、選択したNICモードおよび使用しているサーバのモデルによって異なります。特定のオプションが表示されない場合、そのオプションは選択されているモードまたはサーバ モデルでは使用できません。 次のいずれかになります。 • [アクティブ-アクティブ（active-active）] : サポートされている場合、設定されているNICモードに関連付けられたすべてのポートが同時に動作します。この機能により、スループットが増加し、Cisco IMC への複数のパスが提供されます。 • [アクティブ-スタンバイ（active-standby）] : 設定されているNICモードに関連付けられたポートで障害が発生した場合、トラフィックは、そのNICモードに関連付けられている他のポートの 1 つにフェールオーバーします。 （注） このオプションを選択する場合は、設定されている NIC モードに関連付けられたすべてのポートが同じサブネットに接続され、どのポートが使用されてもトラフィックの安全が保証されるようにする必要があります。
[MACアドレス（MAC Address）] フィールド	[NIC モード（NIC Mode）] フィールドで選択されている Cisco IMC ネットワーク インターフェイスの MAC アドレス。

ステップ 4 [変更の保存（Save Changes）] をクリックします。

共通プロパティの設定

共通プロパティの設定の概要

ホストネーム

ダイナミック ホストコンフィギュレーションプロトコル（DHCP）拡張機能は、ホスト名をDHCPパケットに追加することによって利用でき、DHCP サーバ側でこれを解釈または表示できます。ホスト名はDHCPパケットのオプション フィールドに追加され、最初に DHCP サーバに送信される DHCP DISCOVER パケットで送信されます。

サーバのデフォルトのホスト名は ucs-c2XX から CXXX-YYYYYY に変更されます（XXX はサーバのモデル番号で、YYYYYY はシリアル番号です）。この一意のストリングはクライアント ID として機能し、DHCP サーバから Cisco IMC にリースされる IP アドレスを追跡してマッピングするのに役立ちます。サーバのステッカーまたはラベルとしてデフォルト シリアル番号が製造者から提供され、サーバを識別するのに役立ちます。

ダイナミック DNS

ダイナミック DNS（DDNS）は、Cisco IMC から DNS サーバのリソース レコードを追加または更新するために使用されます。Web UI または CLI を使用してダイナミック DNS をイネーブルにできます。[DDNS] オプションをイネーブルにすると、DDNS サービスは現在のホスト名、ドメイン名、および管理 IP アドレスを記録し、Cisco IMC から DNS サーバのリソース レコードを更新します。

（注） DDNS サーバは、次の DNS 設定のいずれかが変更された場合に、DNS サーバの以前のリソース レコード（もしあれば）を削除し、新しいリソース レコードを追加します。

- ホストネーム
- LDAP 設定のドメイン名
- DDNS と DHCP がイネーブルの場合に、ネットワークまたはサブネットの変更による新しい IP アドレスまたは DNS IP またはドメイン名を DHCP が取得する場合。
- DHCP がディセーブルの場合に、CLI または Web UI を使用してスタティック IP アドレスを設定する場合。
- **dns-use-dhcp** コマンドを入力した場合。

[ダイナミック DNS 更新ドメイン（Dynamic DNS Update Domain）]：ドメインを指定できます。このドメインは、メイン ドメインまたはサブ ドメインのどちらにもできます。このドメイン名は、DDNS 更新のため Cisco IMC のホスト名に付加されます。

共通プロパティの設定

サーバを説明するには、共通プロパティを使用します。

はじめる前に

共通プロパティを設定するには、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 [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [ネットワーキング（Networking）] をクリックします。

ステップ 3 [共通プロパティ（Common Properties）] 領域で、次のプロパティを更新します。

a) [管理ホスト名（Management Hostname）] フィールドに、ホストの名前を入力します。
デフォルトでは、ホスト名は CXXX-YYYYYY 形式で表示されます（XXX はサーバのモデル番号、YYYYYY はシリアル番号です）。

（注） DHCP が有効である場合、発信される DHCP DISCOVER パケットにも Cisco IMC ホスト名が含まれます。

b) [ダイナミック DNS（Dynamic DNS）] チェックボックスをオンにします。

c) [ダイナミック DNS 更新ドメイン（Dynamic DNS Update Domain）] フィールドに、ドメイン名を入力します。

ステップ 4 [変更の保存（Save Changes）] をクリックします。

IPv4 の設定

はじめる前に

IPv4 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 [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [ネットワーキング（Networking）] をクリックします。

ステップ 3 [IPv4 プロパティ（IPv4 Properties）] 領域で、次のプロパティを更新します。

[名前（Name）]	説明
[IPv4 の有効化（Enable IPv4）] チェックボックス	オンにすると、IPv4 がイネーブルになります。
[DHCP の使用（Use DHCP）] チェックボックス	オンにすると、Cisco IMC は DHCP を使用します。
[管理 IP アドレス（Management IP Address）] フィールド	管理 IP アドレス。CMC および BMC の管理に役立つ外部仮想 IP アドレス。
[サブネット マスク（Subnet Mask）] フィールド	IP アドレスのサブネット マスク。
[ゲートウェイ（Gateway）] フィールド	IP アドレスのゲートウェイ。

[名前（Name）]	説明
[DHCP から DNS サーバ アドレスを取得する（Obtain DNS Server Addresses from DHCP）] チェックボックス	オンにすると、Cisco IMC は DNS サーバ アドレスを DHCP から取得します。
[優先 DNS サーバ（Preferred DNS Server）] フィールド	プライマリ DNS サーバの IP アドレス。
[代替 DNS サーバ（Alternate DNS Server）] フィールド	セカンダリ DNS サーバの IP アドレス。

ステップ 4 [変更の保存（Save Changes）] をクリックします。

IPv6 の設定

はじめる前に

IPv6 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 [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [ネットワーキング（Networking）] をクリックします。

ステップ 3 [IPv6 プロパティ（IPv6 Properties）] 領域で、次のプロパティを更新します。

[名前（Name）]	説明
[IPv6 の有効化（Enable IPv6）] チェックボックス	オンにすると、IPv6 がイネーブルになります。
[DHCP の使用（Use DHCP）] チェックボックス	オンにすると、Cisco IMC は DHCP を使用します。 （注） ステートフル DHCP のみがサポートされます。
[管理 IP アドレス（Management IP Address）] フィールド	管理 IPv6 アドレス。 （注） グローバル ユニキャスト アドレスだけがサポートされます。

[名前（Name）]	説明
[プレフィクス長（Prefix Length）] フィールド	IPv6 アドレスのプレフィクス長。値は 1 ～ 127 の範囲で入力します。デフォルト値は 64 です。
[ゲートウェイ（Gateway）] フィールド	IPv6 アドレスのゲートウェイ。 （注） グローバル ユニキャスト アドレスだけがサポートされます。
[DHCP から DNS サーバ アドレスを取得する（Obtain DNS Server Addresses from DHCP）] チェックボックス	オンにすると、Cisco IMC は DNS サーバ アドレスを DHCP から取得します。 （注） [DHCP の使用（Use DHCP）] オプションがイネーブルの場合にのみこのオプションを使用できます。
[優先 DNS サーバ（Preferred DNS Server）] フィールド	プライマリ DNS サーバの IPv6 アドレス。
[代替 DNS サーバ（Alternate DNS Server）] フィールド	セカンダリ DNS サーバの IPv6 アドレス。
[リンク ローカル アドレス（Link Local Address）] フィールド	IPv6 アドレスのリンク ローカル アドレス。

ステップ 4 [変更の保存（Save Changes）] をクリックします。

VLAN への接続

はじめる前に

VLAN に接続するには、admin としてログインしている必要があります。

手順

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

ステップ 2 [管理者（Admin）] メニューの [ネットワーキング（Networking）] をクリックします。

ステップ 3 [VLAN プロパティ（VLAN Properties）] 領域で、次のプロパティを更新します。

[名前（Name）]	説明
[VLAN の有効化（Enable VLAN）] チェックボックス	オンにすると、Cisco IMC は仮想 LAN に接続されます。 （注） VLAN またはポート プロファイルを設定できますが、両方は使用できません。ポート プロファイルを使用する場合は、このチェックボックスがオフになっていることを確認してください。
[VLAN ID] フィールド	VLAN ID。
[優先順位（Priority）] フィールド	VLAN でのこのシステムのプライオリティ。

ステップ 4 [変更の保存（Save Changes）] をクリックします。

ポート プロファイルへの接続

はじめる前に

ポート プロファイルに接続するには、admin としてログインしている必要があります。

手順

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

ステップ 2 [管理者（Admin）] メニューの [ネットワーキング（Networking）] をクリックします。

ステップ 3 [ポート プロパティ（Port Properties）] 領域で、次のプロパティを更新します。

[名前（Name）]	説明
[自動ネゴシエーション（Auto Negotiation）] チェックボックス	このオプションを使用して、スイッチのネットワーク ポート速度とデュプレックス値を設定したり、システムが自動的にスイッチから値を取得できるようにすることができます。このオプションは、専用モードでのみ使用可能です。 • オンにすると、ネットワーク ポート速度とデュプレックスの設定はシステムによって無視され、Cisco IMC はスイッチに設定された速度を保持します。 • オフにした場合は、ネットワーク ポート速度とデュプレックス値を設定できます。

[名前（Name）]	説明
[管理モード（Admin Mode）] 領域	[ネットワーク ポートの速度（Network Port Speed）] フィールド ポートのネットワーク速度。次のいずれかになります。 • 10 Mbps • 100 Mbps • 1 Gbps デフォルト値は、100 Mbps です。[専用（Dedicated）] モードでは、[自動ネゴシエーション（Auto Negotiation）] を無効にすると、ネットワークの速度とデュプレックス値を設定できます。 （注） • ポート速度を変更する前に、接続したスイッチに同じポート速度があることを確認します。 • 1 Gbps のネットワーク ポート速度は、C220 と C240 M3、および C22 と C24 M3 サーバでは使用できません。 [デュプレックス（Duplex）] ドロップダウン リスト Cisco IMC 管理ポートのデュプレックス モード。 次のいずれかになります。 • Half • 完全（Full） デフォルトでは、デュプレックス モードは [フル（Full）] に設定されます。

[名前（Name）]	説明
[操作モード（Operation Mode）] 領域	運用ネットワーク ポート速度とデュプレックス値を表示します。 [自動ネゴシエーション（Auto Negotiation）] チェックボックスをオンにすると、スイッチのネットワーク ポート速度とデュプレックスの詳細が表示されます。オフにした場合は、[管理モード（Admin Mode）] で設定したネットワーク ポート速度とデュプレックス値が表示されます。

ステップ 4 [変更の保存（Save Changes）] をクリックします。

個々の設定の実行

はじめる前に

手順

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

ステップ 2 [管理者（Admin）] メニューの [ネットワーキング（Networking）] をクリックします。

ステップ 3 [個々の設定（Individual Settings）] 領域で、[CMC 1]、[CMC 2]、[BMC 1]、[BMC 2] のそれぞれの領域で次のフィールドを確認し、更新します。

[名前（Name）]	説明
[ホスト名（Hostname）] フィールド	ユーザ定義のホスト名。デフォルトでは、ホスト名は CXXX-YYYYYY 形式で表示されます（XXX はサーバのモデル番号、YYYYYY はシリアル番号です）。
[MACアドレス（MAC Address）] フィールド	コンポーネントの MAC アドレス。
[IPv4 アドレス（IPv4 Address）] フィールド	コンポーネントの IPv4 アドレス。
[IPv6 アドレス（IPv6 Address）] フィールド	コンポーネントの IPv6 アドレス。

[名前（Name）]	説明
[リンク ローカル アドレス（Link Local Address）] フィールド	コンポーネントの IPv6 アドレスのリンク ローカル アドレス。

ステップ 4 [変更の保存（Save Changes）] をクリックします。

次の作業

ネットワーク セキュリティの設定

ネットワーク セキュリティ

Cisco IMC は、IP ブロッキングをネットワーク セキュリティとして使用します。IP ブロッキングは、サーバまたは Web サイトと、特定の IP アドレスまたはアドレス範囲との間の接続を防ぎます。IP ブロッキングは、事実上これらのコンピュータから Web サイト、メール サーバ、またはその他のインターネット サーバへの不要な接続を禁止します。

禁止 IP の設定は、一般的に、サービス拒否（DoS）攻撃から保護するために使用されます。Cisco IMC は、IP ブロッキングの失敗回数を設定して、IP アドレスを禁止します。

ネットワーク セキュリティの設定

IP ブロッキングの失敗回数を設定する場合は、ネットワーク セキュリティを設定します。

はじめる前に

ネットワーク セキュリティを設定するには、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 [管理者（Admin）] メニューをクリックします。

ステップ 2 [ネットワーキング（Networking）] ペインの [ネットワーク セキュリティ（Network Security）] をクリックします。

ステップ 3 [IP ブロッキング プロパティ（IP Blocking Properties）] 領域で、次のプロパティを更新します。

[名前（Name）]	説明
[IP ブロッキングの有効化（Enable IP Blocking）] 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、IP ブロッキングがイネーブルになります。
[IP ブロッキングの失敗回数（IP Blocking Fail Count）] フィールド	指定された時間ユーザがロックアウトされる前に、ユーザが試行できるログインの失敗回数。 このログイン試行失敗の回数は、[IP ブロッキングの失敗ウィンドウ（IP Blocking Fail Window）] フィールドで指定されている期間内に生じる必要があります。 3 ～ 10 の整数を入力します。
[IP ブロッキングの失敗ウィンドウ（IP Blocking Fail Window）] フィールド	ユーザをロックアウトするためにログイン試行の失敗が発生する必要のある期間（秒数）。 60 ～ 120 の整数を入力します。
[IP ブロッキングのペナルティ時間（IP Blocking Penalty Time）] フィールド	ユーザが指定されている期間内にログイン試行の最大回数を超えた場合に、ユーザがロックアウトされている秒数。 300 ～ 900 の整数を入力します。

ステップ 4 [IP フィルタリング（IP Filtering）] 領域で、次のプロパティを更新します。

[名前（Name）]	説明
[IP フィルタリングの有効化（Enable IP Filtering）] チェックボックス	IP フィルタリングをイネーブルにするには、このボックスをオンにします。
[IP フィルタ（IP Filter）] フィールド	サーバへのセキュアなアクセスを提供するために、選択した IP のセットのみにアクセスを許可するフィルタを設定できるようになりました。このオプションでは、IP アドレスを保存するための 4 つのスロット（IP フィルタ 1、2、3、および 4）が提供されます。IP フィルタの設定時に、単一の IP アドレスまたは IP アドレスの範囲を割り当てることができます。IP フィルタを設定すると、他の IP アドレスを使用してサーバにアクセスできなくなります。

ステップ 5 [変更の保存（Save Changes）] をクリックします。

ネットワーク タイム プロトコルの設定

ネットワーク タイム プロトコル サービス設定

デフォルトでは、Cisco IMC がリセットされると、ホストと時刻が同期されます。NTP サービスを導入すると、Cisco IMC を設定して NTP サーバと時刻を同期することができます。デフォルトでは、NTP サーバは Cisco IMC で動作しません。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 サービスをイネーブルにして設定する必要があります。NTP サービスをイネーブルにすると、Cisco IMC は設定された NTP サーバと時刻を同期します。NTP サービスは Cisco IMC でのみ変更できます。

（注） NTP サービスをイネーブルにするには、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。

ネットワーク タイム プロトコル サービスの設定

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。

はじめる前に

このタスクを実行するには、admin 権限で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 [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [ネットワーキング（Networking）] をクリックします。

ステップ 3 [ネットワーキング（Networking）] ペインの [NTP 設定（NTP Setting）] をクリックします。

ステップ 4 [NTP 設定（NTP Settings）] 領域で、次のプロパティを更新します。

[名前（Name）]	説明
NTP を有効にする（Enable NTP）	NTP サービスをイネーブルにするには、このボックスをオンにします。
サーバ 1	NTP サーバまたはタイム ソース サーバとして機能する 4 台のサーバのうちの 1 台の IP/DNS アドレス。
サーバ 2	NTP サーバまたはタイム ソース サーバとして機能する 4 台のサーバのうちの 1 台の IP/DNS アドレス。

[名前（Name）]	説明
サーバ 3	NTP サーバまたはタイム ソース サーバとして機能する 4 台のサーバのうちの 1 台の IP/DNS アドレス。
サーバ 4	NTP サーバまたはタイム ソース サーバとして機能する 4 台のサーバのうちの 1 台の IP/DNS アドレス。
[ステータス（Status）] メッセージ	サーバがリモートの NTP サーバと時刻を同期できるかどうかを示します。次のいずれかになります。 • [ストラタム 7 で NTP サーバ（RefID）に同期（synchronized to NTP server (RefID) at stratum 7）]：NTP サービスが有効で、複数または個々の IPv4 または IPv6 ベースの NTP サーバが追加される場合。 • [非同期（unsynchronized）]：NTP サービスが有効で、不明または到達不能なサーバが追加される場合。 • [NTP サービス無効（NTP service disabled）]：NTP サービスが無効な場合。 （注） ヘルプアイコン上にマウスを移動すると、ストラタムが表すものを説明するポップアップが表示されます。

ステップ 5 [変更の保存（Save Changes）] をクリックします。

第 11 章

ネットワーク アダプタの管理

この章の内容は、次のとおりです。

ネットワーク アダプタのプロパティの表示

はじめる前に

- サーバの電源をオンにする必要があります。そうしないと、プロパティが表示されません。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ネットワーキング（Networking）] メニューをクリックします。

ステップ 2 [ネットワーキング（Networking）] メニューの [アダプタ カード 1（Adapter Card 1）] または [アダプタ カード 2（Adapter Card 2）] をクリックします。

ステップ 3 [アダプタ カードのプロパティ（Adapter Card Properties）] 領域で、次の情報を確認します。

名称	説明
[PCI スロット（PCI Slot）] フィールド	アダプタが装着されている PCI スロット。

名称	説明
[ベンダー（Vendor）] フィールド	アダプタのベンダー。
[製品名（Product Name）] フィールド	アダプタの製品名。
[製品ID（Product ID）] フィールド	アダプタの製品 ID。
[シリアル番号（Serial Number）] フィールド	アダプタのシリアル番号。
[バージョン ID（Version ID）] フィールド	アダプタのバージョン ID。
[ハードウェア リビジョン（Hardware Revision）] フィールド	アダプタのハードウェア リビジョン。
[Cisco IMC 管理の有効化（Cisco IMC Management Enabled）] フィールド	このフィールドに [はい（yes）] と表示されている場合、そのアダプタは Cisco Card モードで動作しており、サーバの Cisco IMC に Cisco IMC 管理トラフィックを渡しています。
[設定の保留（Configuration Pending）] フィールド	このフィールドに [はい（yes）] と表示されている場合、そのアダプタの設定は Cisco IMC で変更されていますが、ホストのオペレーティング システムには変更内容が通知されていません。 変更を有効にするには、管理者がアダプタをリブートする必要があります。
[ISCSI ブート対応（ISCSI Boot Capable）] フィールド	iSCSI ブートがアダプタでサポートされるかどうか。
[CDN 対応（CDN Capable）] フィールド	CDN がアダプタでサポートされるかどうか。
[usNIC 対応（usNIC Capable）] フィールド	アダプタおよびアダプタで実行されるファームウェアが usNIC をサポートするかどうか。
[説明（Description）] フィールド	アダプタのユーザ定義の説明。 1 ～ 63 文字の範囲で入力できます。

名称	説明
[FIP モードの有効化（Enable FIP Mode）] チェックボックス	オンにすると、FCoE Initialization Protocol（FIP）モードがイネーブルになります。FIP モードは、アダプタが現在の FCoE 標準との互換性を保つことを保証します。 （注） このオプションは、テクニカル サポートの担当者から明確に指示された場合にだけ使用してください。
[LLDP の有効化（Enable LLDP）] チェックボックス	オンにすると、Link Layer Discovery Protocol（LLDP）によってすべての Data Center Bridging Capability Exchange プロトコル（DCBX）機能が有効になります。これには、FCoE、プライオリティ ベースのフロー制御も含まれます。 デフォルトで、LLDP オプションは有効になっています。 （注） LLDP オプションを無効にすると、すべての DCBX 機能が無効になるので、このオプションは無効にしないことを推奨します。 （注） このオプションを使用できるのは一部の UCS C シリーズ サーバだけです。
[VNTAG モードの有効化（Enable VNTAG Mode）] チェックボックス	VNTAG モードがイネーブルな場合、以下の操作を実行できます。 • 特定のチャネルに vNIC と vHBA を割り当てる。 • vNIC と vHBA をポート プロファイルに関連付ける。 • 通信に問題が生じた場合、vNIC を他の vNIC にフェールオーバーする。

名称	説明
[ポート 0（Port-0）] ドロップダウン リスト	次のいずれかになります。 • [1 Gbps] • [10 Gbps] • [40 Gbps] • [4 X 10 Gbps] • Auto • [40 Gbps] • 4 x 10 Gbps • [自動（Auto）]：Cisco UCS VIC 13xx（および以降の世代）のアダプタ シリーズでは、値を [自動（Auto）] にすると、ポートに挿入されるトランシーバ モジュールに基づいてアダプタがポートの速度を決定することができます。 （注） 40 Gbps の速度をサポートするアダプタでは、[自動（Auto）] がデフォルトのオプションです。 （注） 40 Gbps スイッチを使用している場合は、ポートの速度として 40 Gbps を選択する必要があります。
[ポート 1（Port-1）] ドロップダウン リスト	次のいずれかになります。 • [1 Gbps] • [10 Gbps] • [40 Gbps] • [4 X 10 Gbps] • Auto • [40 Gbps] • 4 x 10 Gbps • [自動（Auto）]：Cisco UCS VIC 13xx（および以降の世代）のアダプタ シリーズでは、値を [自動（Auto）] にすると、ポートに挿入されるトランシーバ モジュールに基づいてアダプタがポートの速度を決定することができます。 （注） 40 Gbps の速度をサポートするアダプタでは、[自動（Auto）] がデフォルトのオプションです。 （注） 40 Gbps スイッチを使用している場合は、ポートの速度として 40 Gbps を選択する必要があります。

名称	説明
[トレーニング リンク 0（Training Link - 0）] チェックボックス	オンにすると、ポート 0 のリンク トレーニングが有効になります。 （注） ポート 0 で 40 Gbps のポート速度が選択されている場合にのみサポートされます。
[トレーニング リンク 1（Training Link - 1）] チェックボックス	オンにすると、ポート 1 のリンク トレーニングが有効になります。 （注） ポート 1 で 40 Gbps のポート速度が選択されている場合にのみサポートされます。
[PCI リンク（PCI Link）] フィールド	シングル サーバ デュアル SIOC 設定では、[PCI スロット（PCI slot）] フィールドの情報に応じて、サーバに関連付けられているアダプタの vNIC と vHBA が示されます。たとえば、フィールドの値として [PCI スロット（PCI slot）] に 2 が表示され、[PCI リンク（PCI Link）] に Server-1 が表示された場合は、アダプタ 2 の vNIC と vHBA がサーバ 1 ホストに PCI でリンクされていることを示しています。

ステップ 4 [ファームウェア（Firmware）] 領域で、次の情報を確認します。

[名前（Name）]	説明
[稼働バージョン（Running Version）] フィールド	現在有効なファームウェア バージョン。
[バックアップバージョン（Backup Version）] フィールド	アダプタにインストールされている別のファームウェア バージョン（存在する場合）。バックアップ バージョンは現在動作していません。バックアップ バージョンをアクティブにするには、管理者が [アクション（Actions）] 領域で [ファームウェアのアクティブ化（Activate Firmware）] をクリックします。 （注） アダプタに新しいファームウェアをインストールすると、既存のバックアップ バージョンはすべて削除され、新しいファームウェアがバックアップ バージョンになります。アダプタで新しいバージョンを実行するには、その新しいバージョンを手動でアクティブにする必要があります。
[スタートアップバージョン（Startup Version）] フィールド	次回アダプタがリブートされたときにアクティブになるファームウェア バージョン。
[ブートローダーのバージョン（Bootloader Version）] フィールド	アダプタ カードに関連付けられたブートローダのバージョン。

[名前（Name）]	説明
[ステータス（Status）] フィールド	このアダプタで前回実行されたファームウェアのアクティブ化のステータス。 （注） このステータスはアダプタがリブートされるたびにリセットされます。

ステップ 5 [外部イーサネット インターフェイス（External Ethernet Interfaces）] 領域で、次の情報を確認します。

[名前（Name）]	説明
[ID] カラム	アップリンク ポート ID。
[MAC アドレス（MAC Address）] カラム	アップリンク ポートの MAC アドレス。
[リンク ステート（Link State）] カラム	アップリンク ポートの現在の動作状態。次のいずれかになります。 • Fault • リンクアップ（Link Up） • リンクダウン（Link Down） • SFP ID エラー（SFP ID Error） • SFP 未インストール（SFP Not Installed） • SFP セキュリティ チェック失敗（SFP Security Check Failed） • サポートされていない SFP（Unsupported SFP）
[Encap] カラム	アダプタが動作するモード。次のいずれかになります。 • [CE]：クラシカル イーサネット モード。 • [NIV]：ネットワーク インターフェイス仮想化モード。

[名前（Name）]	説明
[管理速度（Admin Speed）] カラム	ポートのデータ転送レート。次のいずれかになります。 • [1 Gbps] • [10 Gbps] • [40 Gbps] • [4 X 10 Gbps] • Auto • [40 Gbps] • [4 X 10 Gbps] （注） 40 Gbps スイッチを使用している場合は、ポートの速度として 40 Gbps を選択する必要があります。
[動作速度（Operating Speed）] カラム	ポートの動作レート。次のいずれかになります。 • [1 Gbps] • [10 Gbps] • [40 Gbps] • [4 X 10 Gbps] • Auto • [40 Gbps] • [4 X 10 Gbps] （注） 40 Gbps スイッチを使用している場合は、ポートの速度として 40 Gbps を選択する必要があります。
[トレーニング リンク（Training Link）] カラム	リンク トレーニングがポートで有効であるかどうかを示します。
[コネクタの有無（Connector Present）] カラム	コネクタがあるかどうかを示します。次のいずれかになります。 • [はい（Yes）] : コネクタが存在します。 • [いいえ（No）] : コネクタが存在しません。 （注） このオプションを使用できるのは一部のアダプタ カードのみです。

[名前（Name）]	説明
[コネクタのサポート（Connector Supported）] カラム	コネクタがシスコによってサポートされているかどうかを示します。次のいずれかになります。 • [はい（Yes）]：コネクタはシスコによってサポートされています。 • [いいえ（No）]：コネクタはシスコによってサポートされていません。 コネクタがサポートされていないと、リンクが起動しません。 （注） このオプションを使用できるのは一部のアダプタ カードのみです。
[コネクタ タイプ（Connector Type）] カラム	コネクタのタイプ。 （注） このオプションを使用できるのは一部のアダプタ カードのみです。
[コネクタ ベンダー（Connector Vendor）] カラム	コネクタのベンダー。 （注） このオプションを使用できるのは一部のアダプタ カードのみです。
[コネクタの製品番号（Connector Part Number）] カラム	コネクタの製品番号。 （注） このオプションを使用できるのは一部のアダプタ カードのみです。
[コネクタの部品リビジョン（Connector Part Revision）] カラム	コネクタの部品のリビジョン番号。 （注） このオプションを使用できるのは一部のアダプタ カードのみです。

ストレージ アダプタのプロパティの表示

はじめる前に

- サーバの電源をオンに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 [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで、適切な LSI MegaRAID または HBA コントローラをクリックします。

ステップ 3 [コントローラ（Controller）] 領域で、[コントローラ情報（Controller Info）] タブがデフォルトで表示されます。

ステップ 4 [作業（Work）] ペインの [ヘルス/ステータス（Health/Status）] 領域で、次の情報を確認します。

[名前（Name）]	説明
[コンポーネントのヘルス（Composite Health）] フィールド	コントローラ、接続されたドライブ、バッテリバックアップユニットの統合ヘルス情報。次のいずれかになります。 • Good • 中程度の障害（Moderate Fault） • 重大な障害（Severe Fault） • 該当なし
[コントローラ ステータス（Controller Status）] フィールド	コントローラの現在のステータス。次のいずれかになります。 • [最適（Optimal）]：コントローラは正常に機能しています。 • [失敗（Failed）]：コントローラが機能していません。 • [無応答（Unresponsive）]：コントローラがダウンしています。
[RAID チップ温度（RAID Chip Temperature）] フィールド	コントローラの温度（摂氏）。
[TTY ログ ステータス（TTY Log Status）] フィールド	TTY ログのダウンロードの現在のステータス。次のいずれかになります。 • [未ダウンロード（Not Downloaded）] • 進行中（In Progress） • 完了

ステップ 5 [ファームウェア バージョン（Firmware Versions）] 領域で、次の情報を確認します。

[名前（Name）]	**説明**
[製品名（Product Name）] フィールド	MegaRAID コントローラの名前。
[シリアル番号（Serial Number）] フィールド	MegaRAID コントローラのシリアル番号。
[ファームウェア パッケージ ビルド（Firmware Package Build）] フィールド	アクティブなファームウェア パッケージのバージョン番号。 ファームウェア コンポーネントのバージョン番号については、[実行中のファームウェア イメージ（Running Firmware Images）] 領域を参照してください。

ステップ 6 [PCI 情報（PCI Info）] 領域で、次の情報を確認します。

[名前（Name）]	**説明**
[PCI スロット（PCI Slot）] フィールド	コントローラが配置されている PCIe スロットの名前。
[ベンダー ID（Vendor ID）] フィールド	PCI ベンダー ID（16 進）。
[デバイス ID（Device ID）] フィールド	PCI デバイス ID（16 進）。
[サブベンダー ID（SubVendor ID）] フィールド	PCI サブベンダー ID（16 進）。
[サブデバイス ID（SubDevice ID）] フィールド	PCI サブデバイス ID（16 進）。

ステップ 7 [製造データ（Manufacturing Data）] 領域で、次の情報を確認します。

[名前（Name）]	**説明**
[製造日（Manufactured Date）] フィールド	MegaRAID カードが製造された日付（yyy-mm-dd 形式）。
[リビジョン番号（Revision No）] フィールド	ボードのリビジョン番号（存在する場合）。

ステップ 8 [ブート ドライブ（Boot Drive）] 領域で、次の情報を確認します。

[名前（Name）]	**説明**
[ブート ドライブ（Boot Drive）] フィールド	ブート ドライブの数。

[名前（Name）]	説明
[ブート ドライブは PD です（Boot Drive is PD）] フィールド	このフィールドに [true] と表示される場合、ブート ドライブは物理ドライブです。

ステップ 9 [実行中のファームウェア イメージ（Running Firmware Images）] 領域で、次の情報を確認します。

[名前（Name）]	説明
[BIOS バージョン（BIOS Version）] フィールド	BIOS オプション PROM のバージョン番号。
[ファームウェアバージョン（Firmware Version）] フィールド	アクティブなファームウェアのバージョン番号。
[プリブート CLI バージョン（Preboot CLI Version）] フィールド	プリブート CLI のバージョン番号。
[WebBIOS バージョン（WebBIOS Version）] フィールド	Web BIOS のバージョン番号。
[NVDATA バージョン（NVDATA Version）] フィールド	不揮発性データ（NVDATA）のバージョン番号。
[ブート ブロック バージョン（Boot Block Version）] フィールド	ブート ブロックのバージョン番号。
[ブート バージョン（Boot Version）] フィールド	LSI コントローラ上のファームウェア ブートローダのバージョン番号。

ステップ 10 [ファームウェア イメージの起動（Startup Firmware Images）] 領域で、次の情報を確認します。

[名前（Name）]	説明
[BIOS バージョンの起動（Startup BIOS Version）] フィールド	ホスト サーバのリブート時にアクティブになる BIOS オプション PROM のバージョン（現在のバージョンと異なる場合）。
[ファームウェア バージョンの起動（Startup Firmware Version）] フィールド	ホスト サーバのリブート時にアクティブになるファームウェア バージョン（現在のバージョンと異なる場合）。
[プリブート CLI バージョンの起動（Startup Preboot CLI Version）] フィールド	ホスト サーバのリブート時にアクティブになるプリブート CLI のバージョン（現在のバージョンと異なる場合）。

[名前（Name）]	説明
[WebBIOS バージョンの起動（Startup WebBIOS Version）] フィールド	ホストサーバのリブート時にアクティブになる Web BIOS のバージョン（現在のバージョンと異なる場合）。
[NVDATA バージョンの起動（Startup NVDATA Version）] フィールド	ホストサーバのリブート時にアクティブになる不揮発性データのバージョン（現在のバージョンと異なる場合）。
[ブート ブロック バージョンの起動（Startup Boot Block Version）] フィールド	ホストサーバのリブート時にアクティブになるブートブロックのバージョン（現在のバージョンと異なる場合）。
[ブート バージョンの起動（Startup Boot Version）] フィールド	ホストサーバのリブート時にアクティブになるファームウェアブートローダのバージョン（現在のバージョンと異なる場合）。

ステップ 11 [仮想ドライブ数（Virtual Drive Count）] 領域で、次の情報を確認します。

[名前（Name）]	説明
[仮想ドライブ数（Virtual Drive Count）] フィールド	コントローラ上で設定されている仮想ドライブの数。
[低下したドライブの数（Degraded Drive Count）] フィールド	コントローラ上の低下状態の仮想ドライブの数。
[オフライン ドライブ数（Offline Drive Count）] フィールド	コントローラ上の障害が発生した仮想ドライブの数。

ステップ 12 [物理ドライブ数（Physical Drive Count）] 領域で、次の情報を確認します。

[名前（Name）]	説明
[ディスク装着数（Disk Present Count）] フィールド	コントローラ上に存在する物理ドライブの数。
[低下したディスク数（Degraded Disk Count）] フィールド	コントローラ上の低下状態の物理ドライブの数。
[失敗したディスク数（Failed Disk Count）] フィールド	コントローラ上の障害が発生した物理ドライブの数。

ステップ 13 [設定（Settings）] 領域で、次の情報を確認します。

[名前（Name）]	説明
[予測障害ポーリング間隔（Predictive Fail Poll Interval）] フィールド	予測障害ポーリングの間隔の秒数。 各ポーリング間に、コントローラはすべての物理ドライブ上の Self-Monitoring Analysis and Reporting Technology（SMART）データを調べ、障害の発生が間近な物理ドライブがあるかどうかを確認します。
[再構築レート（Rebuild Rate）] フィールド	低下した RAID ボリュームをコントローラが再ビルドするレート。 このレートは、使用可能な帯域幅合計に対するパーセンテージで表示されます。
[パトロール読み取りレート（Patrol Read Rate）] フィールド	整合性のないデータを検索するために、コントローラが物理ドライブのバックグラウンド読み取りを実行するレート。 このレートは、使用可能な帯域幅合計に対するパーセンテージで表示されます。
[整合性検査レート（Consistency Check Rate）] フィールド	冗長データの不整合を検索して修正するために、コントローラが仮想ドライブをスキャンするレート。 このレートは、使用可能な帯域幅合計に対するパーセンテージで表示されます。
[再構成レート（Reconstruction Rate）] フィールド	容量または RAID レベルの変更が必要な場合に仮想ドライブが再構築されるレート。 このレートは、使用可能な帯域幅合計に対するパーセンテージで表示されます。
[キャッシュ フラッシュ インターバル（Cache Flush Interval）] フィールド	キャッシュメモリを物理ドライブにフラッシュする前に待機する秒数。
[一度にスピンアップする最大ドライブ数（Max Drives To Spin Up At Once）] フィールド	サーバの電源投入後に同時にスピンアップできるドライブ数。
[スピンアップ グループ間の遅延（Delay Among Spinup Groups）] フィールド	コントローラがドライブの次のセットをスピンアップする前に待機する秒数。

[名前（Name）]	説明
[物理ドライブ強制モード（Physical Drive Coercion Mode）] フィールド	コントローラが物理ドライブのサイズを概数に切り捨てるかどうか。次のいずれかになります。 • [なし（None）]：コントローラは丸めを行いません。 • [128 MB]：ドライブ サイズは最も近い 128 MB の倍数に切り捨てられます。 • [1GB]：ドライブ サイズは最も近い 1GB の倍数に切り捨てられます。
[クラスタ モード（Cluster Mode）] フィールド	このフィールドに [true] と表示される場合、このコントローラ上のドライブは他のサーバのコントローラと共有されます。
[バッテリ警告（Battery Warning）] フィールド	このフィールドに [true] と表示される場合、バッテリ欠落警告はディセーブルです。
[ECC バケット リーク レート（ECC Bucket Leak Rate）] フィールド	エラー訂正コード（ECC）の単一ビットエラー バケット リーク レート（分単位）。 ECC により、コントローラは物理ドライブからの読み取り中に単一ビットエラーを検出したときに、エラー カウンタを増分します。このフィールドで定義された時間（分）が経過するたびに、コントローラはエラー カウンタを減少させます。 エラー カウンタがシステム定義の最大数に達すると、コントローラはイベント メッセージをシステムに送信します。
[ラック デバイスの公開（Expose Enclosure Devices）] フィールド	このフィールドに [true] と表示される場合、ラック デバイスはホスト ドライバに可視です。
[PD 失敗履歴の保持（Maintain PD Fail History）] フィールド	このフィールドに [true] と表示される場合、コントローラは不良と判断された物理ドライブをサーバのリブート間で記憶します。
[SMART でのコピーバックの有効化（Enable Copyback on SMART）] フィールド	このフィールドに [true] と表示される場合、Self-Monitoring Analysis and Reporting Technology（SMART）によってエラーが報告されると、コントローラはドライブの内容をスペア ドライブにコピーします。

[名前（Name）]	説明
[SMART エラーでの SSD へのコピーバックの有効化（Enable Copyback to SSD on SMART Error）] フィールド	このフィールドに [true] と表示される場合、SMART によってエラーが報告されると、コントローラは SSD カードの内容をスペア カードにコピーします。
[ネイティブ コマンド キューイング（Native Command Queuing）] フィールド	このフィールドに [true] と表示される場合、Native Command Queuing（NCQ）はディセーブルです。
[JBOD] フィールド	このフィールドに [true] と表示される場合、JBOD はイネーブルです。
[未設定ドライブのスピンダウンの有効化（Enable Spin Down of Unconfigured Drives）] フィールド	このフィールドに [true] と表示される場合、コントローラは未設定のドライブをスピンダウンします。
[SSD パトロール読み取りの有効化（Enable SSD Patrol Read）] フィールド	このフィールドに [true] と表示される場合、コントローラは SSD カードでパトロール読み取りを実行します。
[自動向上インポート（Auto Enhanced Import）] フィールド	このフィールドに [true] と表示される場合、コントローラのブート時に外部設定が自動的にインポートされます。

ステップ 14 [機能（Capabilities）] 領域で、次の情報を確認します。

[名前（Name）]	説明
[サポートされる RAID レベル（RAID Levels Supported）] フィールド	コントローラでサポートされる RAID レベル。次の中から 1 つ以上選択できます。 • [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 1E]：統合オフセット ストライプ ミラーリング • [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]：パリティ付きのスパンされたストライピング。 • [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 srl-03]：スパンされたセカンダリ RAID レベル • [Raid 00]：スパンされたストライピング。 • [Raid 1e-rlq0]：スパンを使用しない統合隣接ストライプ ミラーリング。 • [Raid 1e0-rlq0]：スパンを使用する統合隣接ストライプ ミラーリング。

ステップ 15 [HW 設定（HW Configuration）] 領域で、次の情報を確認します。

[名前（Name）]	説明
[SAS アドレス（SAS Address）] フィールド	MegaRAID コントローラは、最大 16 個のシリアル接続 SCSI（SAS）アドレスを持つことができます。このフィールドには、最初の 8 個の SAS アドレス（使用中の場合）が表示されます。
[BBU の有無（BBU Present）] フィールド	このフィールドに [true] と表示される場合、バッテリ バックアップ ユニットが存在します。

[名前（Name）]	説明
[NVRAM の有無（NVRAM Present）] フィールド	このフィールドに [true] と表示される場合、NVRAM が存在します。
[NVRAM サイズ（NVRAM Size）] フィールド	NVRAM のサイズ（KB 単位）。
[シリアル デバッガの有無（Serial Debugger Present）] フィールド	このフィールドに [true] と表示される場合、シリアルデバッガが RAID カードに接続されています。
[メモリの有無（Memory Present）] フィールド	このフィールドに [true] と表示される場合、メモリが存在します。
[フラッシュの有無（Flash Present）] フィールド	このフィールドに [true] と表示される場合、フラッシュ メモリが存在します。
[フラッシュ サイズ（Flash Size）] フィールド	フラッシュ メモリのサイズ（MB 単位）。
[メモリ サイズ（Memory Size）] フィールド	メモリのサイズ（MB 単位）。
[キャッシュ メモリ サイズ（Cache Memory Size）] フィールド	キャッシュ メモリのサイズ（MB 単位）。
[バックエンド ポートの数（Number of Backend Ports）] フィールド	コントローラ上の SATA または SAS ポートの数。

ステップ 16 [エラー カウンタ（Error Counters）] 領域で、次の情報を確認します。

[名前（Name）]	説明
[メモリの修正可能なエラー数（Memory Correctable Errors）] フィールド	コントローラ メモリ内の修正可能なエラーの数。
[メモリの修正不可能なエラー数（Memory Uncorrectable Errors）] フィールド	コントローラ メモリ内の修正不可能なエラーの数。

vHBA の管理

vHBA 管理のガイドライン

vHBA を管理する場合は、次のガイドラインと制限事項を考慮してください。

- Cisco UCS P81E 仮想インターフェイス カード および Cisco UCS VIC 1225 仮想インターフェイス カード には 2 つの vHBA（fc0 と fc1）があります。これらのアダプタ カードに追加の vHBA を最大 16 個まで作成できます。

（注） アダプタに対してネットワーク インターフェイスの仮想化（NIV）モードがイネーブルになっている場合は、vHBA を作成するときにチャネル番号を割り当てる必要があります。

- FCoE アプリケーションで Cisco UCS P81E 仮想インターフェイス カード または Cisco UCS VIC 1225 仮想インターフェイス カード を使用する場合は、vHBA を FCoE VLAN に関連付ける必要があります。VLAN を割り当てるには、「vHBA のプロパティの変更」で説明されている手順に従います。
- 設定の変更後は、その設定を有効にするためにホストをリブートする必要があります。

vHBA のプロパティの表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ネットワーキング（Networking）] メニューをクリックします。

ステップ 2 [アダプタ カード（Adapter Card）] ペインの [vHBAs] タブをクリックします。

ステップ 3 [vHBAs] ペインの [fc0] または [fc1] をクリックします。

ステップ 4 [vHBA プロパティ（vHBA Properties）] の [全般（General）] 領域で、次のフィールドの情報を確認します。

[名前（Name）]	説明
[名前（Name）] フィールド	仮想 HBA の名前。 この名前は、vHBA の作成後は変更できません。

[名前（Name）]	説明
[ターゲット WWNN（Target WWNN）] フィールド	vHBA に関連付けられた WWNN。 WWNN を自動的に生成するには、[自動（AUTO）] を選択します。WWNN を指定するには、2 つ目のオプション ボタンをクリックし、対応するフィールドに WWNN を入力します。
[ターゲット WWPN（Target WWPN）] フィールド	vHBA に関連付けられた WWPN。 WWPN を自動的に生成するには、[自動（AUTO）] を選択します。WWPN を指定するには、2 つ目のオプション ボタンをクリックし、対応するフィールドに WWPN を入力します。
[FC SAN ブート（FC SAN Boot）] チェックボックス	オンにすると、vHBA を使用して SAN ブートを実行できます。
[永続的 LUN のバインドの有効化（Enable Persistent LUN Binding）] チェックボックス	オンにすると、LUN ID のアソシエーションは手動でクリアされるまで、メモリに維持されます。
[アップリンク ポート（Uplink Port）] フィールド	vHBA に関連付けられたアップリンク ポート。 （注） この値は、システム定義の vHBA である fc0 と fc1 については変更できません。
[MACアドレス（MAC Address）] フィールド	vHBA に関連付けられた MAC アドレス。 システムが MAC アドレスを生成するようにするには、[自動（AUTO）] を選択します。アドレスを指定するには、2 番目のオプション ボタンをクリックし、対応するフィールドに MAC アドレスを入力します。
[デフォルト VLAN（Default VLAN）] フィールド	この vHBA にデフォルトの VLAN がない場合、[なし（NONE）] をクリックします。それ以外の場合は、2 つ目のオプション ボタンをクリックし、フィールドに 1 ～ 4094 の VLAN ID を入力します。
[サービス クラス（Class of Service）] ドロップダウン リスト	vHBA の CoS。 0 ～ 6 の整数を選択します。0 が最も低い優先度で、6 が最も高い優先度になります。 （注） このオプションは VNTAG モードでは使用できません。

[名前（Name）]	説明
[レート制限（Rate Limit）] フィールド	この vHBA 上のトラフィックのデータ レート制限（Mbps 単位）。 この vHBA に無制限のデータ レートを設定するには、[オフ（OFF）] を選択します。それ以外の場合は、2 つ目のオプション ボタンをクリックし、1 ～ 10,000 の整数を入力します。 （注） このオプションは VNTAG モードでは使用できません。
[PCIe デバイスの順序（PCIe Device Order）] フィールド	この vHBA が使用される順序。 システムが順序を設定するようにするには、[いずれか（ANY）] を選択します。順序を指定する場合、2 つ目のオプション ボタンを選択し、0 ～ 17 の整数を入力します。
[EDTOV] フィールド	エラー検出タイムアウト値（EDTOV）。システムが、エラーが発生したと見なすまでに待機するミリ秒数です。 1,000 ～ 100,000 の整数を入力します。デフォルトは 2,000 ミリ秒です。
[RATOV] フィールド	リソース割り当てタイムアウト値（RATOV）。システムが、リソースを適切に割り当てることができないと見なすまでに待機するミリ秒数です。 5,000 ～ 100,000 の整数を入力します。デフォルトは 10,000 ミリ秒です。
[データフィールドの最大サイズ（Max Data Field Size）] フィールド	vHBA がサポートするファイバ チャネル フレームのペイロード バイトの最大サイズ。 256 ～ 2112 の整数を入力します。
[チャネル番号（Channel Number）] フィールド	この vHBA に割り当てるチャネル番号。 1 ～ 1,000 の整数を入力します。 （注） このオプションには VNTAG モードが必要です。
[ポート プロファイル（Port Profile）] ドロップダウン リスト	vHBA に関連付ける必要があるポート プロファイル（ある場合）。 このフィールドには、このサーバが接続しているスイッチに定義されたポート プロファイルが表示されます。 （注） このオプションには VNTAG モードが必要です。

ステップ 5 [エラー リカバリ（Error Recovery）] 領域で、次のフィールドの情報を確認します。

[名前（Name）]	説明
[FCP エラー リカバリの有効化（Enable FCP Error Recovery）] チェックボックス	オンにすると、システムは FCP Sequence Level Error Recovery プロトコル（FC-TAPE）を使用します。
[リンクダウンタイムアウト（Link Down Timeout）] フィールド	アップリンク ポートがダウンし、ファブリック接続が失われていることをシステムに通知する前に、アップリンク ポートがオフラインになっていなければならないミリ秒数。 0 ～ 240,000 の整数を入力します。
[ポート ダウン IO の再試行（Port Down I/O Retries）] フィールド	ポートが使用不可能であるとシステムが判断する前に、そのポートへの I/O 要求がビジー状態を理由に戻される回数。 0 ～ 255 の整数を入力します。
[I/O タイムアウトの再試行（I/O Timeout Retry）] フィールド	再試行までにシステムがタイムアウトを待機する時間。定義されたタイムアウト時間内にディスクが I/O に応答しなかった場合、ドライバは保留中のコマンドを破棄し、タイマーが期限切れになった後に同じ I/O を再送信します。 1 ～ 59 の整数を入力します。
[ポートダウンタイムアウト（Port Down Timeout）] フィールド	リモート ファイバ チャネル ポートが使用不可能であることを SCSI 上位層に通知する前に、そのポートがオフラインになっていなければならないミリ秒数。 0 ～ 240,000 の整数を入力します。

ステップ 6 [ファイバ チャネル割り込み（Fibre Channel Interrupt）] 領域で、次のフィールドの情報を確認します。

[名前（Name）]	説明
[割り込みモードの選択（Interrupt Mode）] ドロップダウン リスト	優先ドライバ割り込みモード。次のいずれかになります。 • [MSIx]：機能拡張された Message Signaled Interrupts（MSI）。これは推奨オプションです。 • [MSI]：MSI のみ。 • [INTx]：PCI INTx 割り込み。

ステップ 7 [ファイバ チャネル ポート（Fibre Channel Port）] 領域で、次のフィールドの情報を確認します。

[名前（Name）]	説明
[IO スロットル数（I/O Throttle Count）] フィールド	vHBA 内に同時に保留可能な I/O 操作の数。 1 ～ 1,024 の整数を入力します。
[ターゲットあたりの LUN 数（LUNs Per Target）] フィールド	ドライバでエクスポートされる LUN の最大数。通常は、オペレーティング システム プラットフォームの制限です。 1 ～ 1,024 の整数を入力します。推奨値は 1024 です。
[LUN キューの深さ（LUN Queue Depth）] フィールド	HBA が 1 つのチャンクで送受信できる LUN ごとのコマンドの数。このパラメータにより、アダプタのすべての LUN について初期キューの深さを調整します。 デフォルト値は、20（物理ミニポートの場合）と 250（仮想ミニポートの場合）です。

ステップ 8 [ファイバ チャネル ポート FLOGI（Fibre Channel Port FLOGI）] 領域で、次のフィールドの情報を確認します。

[名前（Name）]	説明
[FLOGI の再試行回数（FLOGI Retries）] フィールド	システムがファブリックへのログインを最初に失敗してから再試行する回数。 再試行回数を無制限に指定するには、[無制限（INFINITE）] オプション ボタンを選択します。それ以外の場合は、2 番目のオプション ボタンを選択し、対応するフィールドに整数を入力します。
[FLOGI タイムアウト（FLOGI Timeout）] フィールド	システムがログインを再試行する前に待機するミリ秒数。 1,000 ～ 255,000 の整数を入力します。

ステップ 9 [ファイバ チャネル ポート PLOGI（Fibre Channel Port PLOGI）] 領域で、次のフィールドの情報を確認します。

[名前（Name）]	説明
[PLOGI の再試行回数] フィールド	システムがポートへのログインを最初に失敗してから再試行する回数。 0 ～ 255 の整数を入力します。
[PLOGI タイムアウト（PLOGI Timeout）] フィールド	システムがログインを再試行する前に待機するミリ秒数。 1,000 ～ 255,000 の整数を入力します。

ステップ 10 [SCSI I/O] 領域で、次のフィールドの情報を確認します。

[名前（Name）]	説明
[CDB 送信キュー数（CDB Transmit Queue Count）] フィールド	システムで割り当てる SCSI I/O キュー リソースの数。 1 ～ 8 の整数を入力します。
[CDB 送信キュー リング サイズ（CDB Transmit Queue Ring Size）] フィールド	各 SCSI I/O キュー内の記述子の数。 64 ～ 512 の整数を入力します。

ステップ 11 [送受信キュー（Receive/Transmit Queues）] 領域で、次のフィールドの情報を確認します。

[名前（Name）]	説明
[FC ワーク キュー リング サイズ（FC Work Queue Ring Size）] フィールド	各送信キュー内の記述子の数。 64 ～ 128 の整数を入力します。
[FC 受信キュー リング サイズ（FC Receive Queue Ring Size）] フィールド	各受信キュー内の記述子の数。 64 ～ 128 の整数を入力します。

vHBA のプロパティの変更

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ネットワーキング（Networking）] メニューをクリックします。

ステップ 2 [アダプタ カード（Adapter Card）] ペインの [vHBAs] タブをクリックします。

ステップ 3 [vHBAs] ペインの [fc0] または [fc1] をクリックします。

ステップ 4 [全般（General）] 領域で、次のフィールドを更新します。

[名前（Name）]	説明
[名前（Name）] フィールド	仮想 HBA の名前。 この名前は、vHBA の作成後は変更できません。

[名前（Name）]	説明
[ターゲット WWNN（Target WWNN）] フィールド	vHBA に関連付けられた WWNN。 WWNN を自動的に生成するには、[自動（AUTO）] を選択します。WWNN を指定するには、2 つ目のオプション ボタンをクリックし、対応するフィールドに WWNN を入力します。
[ターゲット WWPN（Target WWPN）] フィールド	vHBA に関連付けられた WWPN。 WWPN を自動的に生成するには、[自動（AUTO）] を選択します。WWPN を指定するには、2 つ目のオプション ボタンをクリックし、対応するフィールドに WWPN を入力します。
[FC SAN ブート（FC SAN Boot）] チェックボックス	オンにすると、vHBA を使用して SAN ブートを実行できます。
[永続的 LUN のバインドの有効化（Enable Persistent LUN Binding）] チェックボックス	オンにすると、LUN ID のアソシエーションは手動でクリアされるまで、メモリに維持されます。
[アップリンク ポート（Uplink Port）] フィールド	vHBA に関連付けられたアップリンク ポート。 （注） この値は、システム定義の vHBA である fc0 と fc1 については変更できません。
[MACアドレス（MAC Address）] フィールド	vHBA に関連付けられた MAC アドレス。 システムが MAC アドレスを生成するようにするには、[自動（AUTO）] を選択します。アドレスを指定するには、2 番目のオプション ボタンをクリックし、対応するフィールドに MAC アドレスを入力します。
[デフォルト VLAN（Default VLAN）] フィールド	この vHBA にデフォルトの VLAN がない場合、[なし（NONE）] をクリックします。それ以外の場合は、2 つ目のオプション ボタンをクリックし、フィールドに 1 ～ 4094 の VLAN ID を入力します。
[サービス クラス（Class of Service）] ドロップダウン リスト	vHBA の CoS。 0 ～ 6 の整数を選択します。0 が最も低い優先度で、6 が最も高い優先度になります。 （注） このオプションは VNTAG モードでは使用できません。

[名前（Name）]	説明
[レート制限（Rate Limit）] フィールド	この vHBA 上のトラフィックのデータ レート制限（Mbps 単位）。 この vHBA に無制限のデータ レートを設定するには、[オフ（OFF）] を選択します。それ以外の場合は、2 つ目のオプション ボタンをクリックし、1 ～ 10,000 の整数を入力します。 （注） このオプションは VNTAG モードでは使用できません。
[PCIe デバイスの順序（PCIe Device Order）] フィールド	この vHBA が使用される順序。 システムが順序を設定するようにするには、[いずれか（ANY）] を選択します。順序を指定する場合、2 つ目のオプション ボタンを選択し、0 ～ 17 の整数を入力します。
[EDTOV] フィールド	エラー検出タイムアウト値（EDTOV）。システムが、エラーが発生したと見なすまでに待機するミリ秒数です。 1,000 ～ 100,000 の整数を入力します。デフォルトは 2,000 ミリ秒です。
[RATOV] フィールド	リソース割り当てタイムアウト値（RATOV）。システムが、リソースを適切に割り当てることができないと見なすまでに待機するミリ秒数です。 5,000 ～ 100,000 の整数を入力します。デフォルトは 10,000 ミリ秒です。
[データフィールドの最大サイズ（Max Data Field Size）] フィールド	vHBA がサポートするファイバ チャネル フレームのペイロード バイトの最大サイズ。 256 ～ 2112 の整数を入力します。
[チャネル番号（Channel Number）] フィールド	この vHBA に割り当てるチャネル番号。 1 ～ 1,000 の整数を入力します。 （注） このオプションには VNTAG モードが必要です。
[ポート プロファイル（Port Profile）] ドロップダウン リスト	vHBA に関連付ける必要があるポート プロファイル（ある場合）。 このフィールドには、このサーバが接続しているスイッチに定義されたポート プロファイルが表示されます。 （注） このオプションには VNTAG モードが必要です。

ステップ 5 [エラー リカバリ（Error Recovery）] 領域で、次のフィールドを更新します。

[名前（Name）]	説明
[FCP エラー リカバリの有効化（Enable FCP Error Recovery）] チェックボックス	オンにすると、システムは FCP Sequence Level Error Recovery プロトコル（FC-TAPE）を使用します。
[リンクダウンタイムアウト（Link Down Timeout）] フィールド	アップリンク ポートがダウンし、ファブリック接続が失われていることをシステムに通知する前に、アップリンク ポートがオフラインになっていなければならないミリ秒数。 0 ～ 240,000 の整数を入力します。
[ポート ダウン IO の再試行（Port Down I/O Retries）] フィールド	ポートが使用不可能であるとシステムが判断する前に、そのポートへの I/O 要求がビジー状態を理由に戻される回数。 0 ～ 255 の整数を入力します。
[I/O タイムアウトの再試行（I/O Timeout Retry）] フィールド	再試行までにシステムがタイムアウトを待機する時間。定義されたタイムアウト時間内にディスクが I/O に応答しなかった場合、ドライバは保留中のコマンドを破棄し、タイマーが期限切れになった後に同じ I/O を再送信します。 1 ～ 59 の整数を入力します。
[ポートダウンタイムアウト（Port Down Timeout）] フィールド	リモート ファイバ チャネル ポートが使用不可能であることを SCSI 上位層に通知する前に、そのポートがオフラインになっていなければならないミリ秒数。 0 ～ 240,000 の整数を入力します。

ステップ 6 [ファイバ チャネル割り込み（Fibre Channel Interrupt）] 領域で、次のフィールドを更新します。

[名前（Name）]	説明
[割り込みモードの選択（Interrupt Mode）] ドロップダウン リスト	優先ドライバ割り込みモード。次のいずれかになります。 • [MSIx]：機能拡張された Message Signaled Interrupts（MSI）。これは推奨オプションです。 • [MSI]：MSI のみ。 • [INTx]：PCI INTx 割り込み。

ステップ 7 [ファイバ チャネル ポート（Fibre Channel Port）] 領域で、次のフィールドを更新します。

[名前（Name）]	説明
[IO スロットル数（I/O Throttle Count）] フィールド	vHBA 内に同時に保留可能な I/O 操作の数。 1 ～ 1,024 の整数を入力します。
[ターゲットあたりの LUN 数（LUNs Per Target）] フィールド	ドライバでエクスポートされる LUN の最大数。通常は、オペレーティング システム プラットフォームの制限です。 1 ～ 1,024 の整数を入力します。推奨値は 1024 です。
[LUN キューの深さ（LUN Queue Depth）] フィールド	HBA が 1 つのチャンクで送受信できる LUN ごとのコマンドの数。このパラメータにより、アダプタのすべての LUN について初期キューの深さを調整します。 デフォルト値は、20（物理ミニポートの場合）と 250（仮想ミニポートの場合）です。

ステップ 8 [ファイバ チャネル ポート FLOGI（Fibre Channel Port FLOGI）] 領域で、次のフィールドを更新します。

[名前（Name）]	説明
[FLOGI の再試行回数（FLOGI Retries）] フィールド	システムがファブリックへのログインを最初に失敗してから再試行する回数。 再試行回数を無制限に指定するには、[無制限（INFINITE）] オプション ボタンを選択します。それ以外の場合は、2 番目のオプション ボタンを選択し、対応するフィールドに整数を入力します。
[FLOGI タイムアウト（FLOGI Timeout）] フィールド	システムがログインを再試行する前に待機するミリ秒数。 1,000 ～ 255,000 の整数を入力します。

ステップ 9 [ファイバ チャネル ポート PLOGI（Fibre Channel Port PLOGI）] 領域で、次のフィールドを更新します。

[名前（Name）]	説明
[PLOGI の再試行回数] フィールド	システムがポートへのログインを最初に失敗してから再試行する回数。 0 ～ 255 の整数を入力します。
[PLOGI タイムアウト（PLOGI Timeout）] フィールド	システムがログインを再試行する前に待機するミリ秒数。 1,000 ～ 255,000 の整数を入力します。

ステップ 10 [SCSI I/O] 領域で、次のフィールドを更新します。

[名前（Name）]	説明
[CDB 送信キュー数（CDB Transmit Queue Count）] フィールド	システムで割り当てる SCSI I/O キュー リソースの数。 1 ～ 8 の整数を入力します。
[CDB 送信キュー リング サイズ（CDB Transmit Queue Ring Size）] フィールド	各 SCSI I/O キュー内の記述子の数。 64 ～ 512 の整数を入力します。

ステップ 11 [送受信キュー（Receive/Transmit Queues）] 領域で、次のフィールドを更新します。

[名前（Name）]	説明
[FC ワーク キュー リング サイズ（FC Work Queue Ring Size）] フィールド	各送信キュー内の記述子の数。 64 ～ 128 の整数を入力します。
[FC 受信キュー リング サイズ（FC Receive Queue Ring Size）] フィールド	各受信キュー内の記述子の数。 64 ～ 128 の整数を入力します。

ステップ 12 [変更の保存（Save Changes）] をクリックします。

vHBA の作成

アダプタは 2 つの固定 vHBA を備えています。NIV モードがイネーブルの場合、最大 16 個の追加 vHBA を作成できます。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ネットワーキング（Networking）] メニューをクリックします。

ステップ 2 [アダプタ カード（Adapter Card）] ペインの [vHBAs] タブをクリックします。

ステップ 3 [ホスト ファイバー チャネル インターフェイス（Host Fibre Channel Interfaces）] 領域で、次のアクションのいずれかを選択します。

- デフォルトの設定を使用して vHBA を作成するには、[vHBA の追加（Add vHBA）] をクリックします。

- 既存の vHBA と同じ設定を使用して vHBA を作成するには、その vHBA を選択して [vHBA の複製（Clone vHBA）] をクリックします。

[vHBA の追加（Add vHBA）] ダイアログボックスが表示されます。

ステップ 4 [vHBA の追加（Add vHBA）] ダイアログボックスで、vHBA の名前を 名前 入力ボックスに入力します。

ステップ 5 [vHBA の追加（Add vHBA）] をクリックします。

次の作業

- サーバをリブートして vHBA を作成します。
- 設定の変更が必要な場合は、vHBA のプロパティの変更, （203 ページ） の説明に従って、新しい vHBA を設定します。

vHBA の削除

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ネットワーキング（Networking）] メニューをクリックします。

ステップ 2 [アダプタ カード（Adapter Card）] ペインの [vHBAs] タブをクリックします。

ステップ 3 [ホスト ファイバー チャネル インターフェイス（Host Fibre Channel Interfaces）] 領域で、表から vHBA（複数可）を選択します。

（注） 2 つのデフォルトの vHBA である [fc0] または [fc1] は削除できません。

ステップ 4 [vHBA の削除（Delete vHBAs）] をクリックし、[OK] をクリックして確認します。

vHBA ブート テーブル

vHBA ブート テーブルには、サーバがブート可能な LUN を 4 つまで指定できます。

ブート テーブル エントリの作成

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ネットワーキング（Networking）] メニューをクリックします。

ステップ 2 [アダプタ カード（Adapter Card）] ペインの [vHBAs] タブをクリックします。

ステップ 3 [ファイバー チャネル インターフェイス（Fibre Channel Interfaces）] 領域で、[ブート テーブル（Boot Table）] 領域までスクロール ダウンします。

ステップ 4 [ブート エントリの追加（Add Boot Entry）] ボタンをクリックして [ブート エントリの追加（Add Boot Entry）] ダイアログボックスを開きます。

ステップ 5 [ブート エントリの追加（Add Boot Entry）] ダイアログボックスで、次の情報を確認し、指定された操作を実行します。

[名前（Name）]	説明
[ターゲット WWPN（Target WWPN）] フィールド	ブート イメージの場所に対応するワールド ワイド ポート（WWPN）名。 WWPN は hh:hh:hh:hh:hh:hh:hh:hh の形式で入力します。
[LUN ID] フィールド	ブート イメージの場所に対応する LUN ID。 ID として 0 ～ 255 の値を入力します。
[ブート エントリの追加（Add Boot Entry）] ボタン	指定された場所をブート テーブルに追加します。
[値のリセット（Reset Values）] ボタン	現在フィールドに入力されている値をクリアします。
[キャンセル（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。

ブート テーブル エントリの削除

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ネットワーキング（Networking）] メニューをクリックします。

ステップ 2 [アダプタ カード（Adapter Card）] ペインの [vHBAs] タブをクリックします。

ステップ 3 [ファイバー チャネル インターフェイス（Fibre Channel Interfaces）] 領域で、[ブート テーブル（Boot Table）] 領域までスクロール ダウンします。

ステップ 4 [ブート テーブル（Boot Table）] 領域で、削除するエントリをクリックします。

ステップ 5 [ブート エントリの削除（Delete Boot Entry）] をクリックし、[OK] をクリックして確認します。

vHBA の永続的なバインディング

永続的なバインディングは、システムによって割り当てられたファイバ チャネル ターゲットのマッピングがリブート後も維持されることを保証します。

永続的なバインディングの表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ネットワーキング（Networking）] メニューをクリックします。

ステップ 2 [アダプタ カード（Adapter Card）] ペインの [vHBAs] タブをクリックします。

ステップ 3 [vHBAs] ペインの [fc0] または [fc1] をクリックします。

ステップ 4 [永続的なバインディング（Persistent Bindings）] ダイアログボックスで、次の情報を確認します。

[名前（Name）]	説明
[インデックス（Index）] カラム	バインディングの固有識別子。
[ターゲット WWPN（Target WWPN）] カラム	バインディングが関連付けられるターゲットのワールドワイドポート名。
[ホスト WWPN（Host WWPN）] カラム	バインディングが関連付けられるホストのワールドワイドポート名。

[名前（Name）]	説明
[バス ID（Bus ID）] カラム	バインディングが関連付けられるバス ID。
[ターゲット ID（Target ID）] カラム	バインディングが関連付けられる、ホスト システム上のターゲット ID。
[永続的なバインディングの再構築（Rebuild Persistent Bindings）] ボタン	未使用のすべてのバインディングをクリアし、使用されているバインディングをリセットします。
[閉じる（Close）] ボタン	ダイアログボックスを閉じ、変更を保存します。

ステップ 5 [閉じる（Close）] をクリックします。

永続的なバインディングの再作成

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ネットワーキング（Networking）] メニューをクリックします。

ステップ 2 [アダプタ カード（Adapter Card）] ペインの [vHBAs] タブをクリックします。

ステップ 3 [vHBAs] ペインの [fc0] または [fc1] をクリックします。

ステップ 4 [ファイバー チャネル インターフェイス（Fibre Channel Interfaces）] 領域で、[永続的なバインディング（Persistent Bindings）] 領域までスクロール ダウンします。

ステップ 5 [永続的なバインディングの再構築（Rebuild Persistent Bindings）] ボタンをクリックします。

ステップ 6 [OK] をクリックして確認します。

vNIC の管理

vNIC 管理のガイドライン

vNIC を管理する場合は、次のガイドラインと制限事項を考慮してください。

- Cisco UCS P81E 仮想インターフェイス カード および Cisco UCS VIC 1225 仮想インターフェイス カード には 2 つのデフォルト vNIC（eth0 と eth1）があります。これらのアダプタ カードに最大 16 個の追加 vNIC を作成できます。

（注） アダプタに対してネットワーク インターフェイスの仮想化（NIV）モードがイネーブルになっている場合、vNIC を作成するときにチャネル番号を割り当てる必要があります。

- 設定の変更後は、その設定を有効にするためにホストをリブートする必要があります。

Cisco C シリーズ サーバは、パケット転送に Remote Direct Memory Access（RDMA）over Converged Ethernet（RoCE）を使用します。RoCE では、RDMA over InfiniBand と同様のメカニズムをベースにイーサネットでの RDMA 実行メカニズムを定義しています。ただし、低遅延、低 CPU 使用率、およびネットワーク帯域幅の高利用率というパフォーマンス指向の特性を伴う RoCE は、従来のネットワーク ソケット実装よりも優れたパフォーマンスを提供します。RoCE は、ネットワークで大量のデータを極めて効率的に移動するという要件を満たします。

vNIC のパフォーマンスを向上させるには、Cisco UCS Manager で RoCE ファームウェアに次の設定パラメータを指定する必要があります。

- キュー ペア（Queue Pairs）
- メモリ領域（Memory Regions）
- リソース グループ

RoCE を搭載した SMB ダイレクトのガイドラインと制約事項

- RoCE を搭載した Microsoft SMB ダイレクトは次でサポートされています。
  - Windows 2012 R2。
  - Windows 2016。
- Cisco UCS C シリーズ サーバでは、RoCE 対応 vNIC をアダプタごとに 4 つまでしかサポートしません。
- Cisco UCS C シリーズ サーバでは、NVGRE、VXLAN、VMQ、または usNIC での RoCE をサポートしません。
- アダプタごとのキュー ペアの最大数は 8192 個です。
- アダプタごとのメモリ領域の最大数は 524288 個です。
- Cisco アダプタ間での RoCE 構成はサポートされています。Cisco アダプタとサード パーティ製のアダプタ間の相互運用性はサポートされていません。

重要 RDMA トラフィック パス内のスイッチでドロップなし QOS ポリシーの設定を構成する必要があります。

vNIC のプロパティの表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ネットワーキング（Networking）] メニューをクリックします。

ステップ 2 [アダプタ カード（Adapter Card）] ペインの [vNICs] タブをクリックします。

ステップ 3 [vNICs] ペインの [eth0] または [eth1] をクリックします。

ステップ 4 [イーサネット インターフェイス（Ethernet Interfaces）] ペインの [vNIC プロパティ（vNIC Properties）] 領域で、次のフィールドの情報を確認します。

名称	説明
[名前（Name）] フィールド	仮想 NIC の名前。 この名前は、vNIC の作成後は変更できません。
[CDN] フィールド	VIC カードのイーサネット vNIC に割り当てることができる一貫したデバイス名（CDN）。特定の CDN をデバイスに割り当てることで、ホスト OS 上でそれを識別できます。 （注） この機能は、[VIC に対する CDN サポート（CDN Support for VIC）] トークンが BIOS で有効になっている場合にのみ機能します。
[MTU] フィールド	この vNIC で受け入れられる最大伝送単位、つまりパケット サイズ。 1500 ～ 9000 の整数を入力します。
[アップリンク ポート（Uplink Port）] ドロップダウン リスト	この vNIC に関連付けられたアップリンク ポート。この vNIC に対するすべてのトラフィックは、このアップリンク ポートを通過します。
[MACアドレス（MAC Address）] フィールド	vNIC に関連付けられた MAC アドレス。 アダプタが内部プールから使用可能な MAC アドレスを選択するようにするには、[自動（Auto）] を選択します。アドレスを指定するには、2 番目のオプション ボタンをクリックし、対応するフィールドに MAC アドレスを入力します。

名称	説明
[サービス クラス（Class of Service）] ドロップダウン リスト	この vNIC からのトラフィックに関連付けられるサービス クラス。 0 ～ 6 の整数を選択します。0 が最も低い優先度で、6 が最も高い優先度になります。 （注） このオプションは VNTAG モードでは使用できません。
[信頼ホスト CoS（Trust Host CoS）] チェックボックス	vNIC で、ホスト オペレーティング システムが提供するサービス クラスを使用できるようにするには、このチェックボックスをオンにします。
[PCI 順序（PCI Order）] フィールド	この vNIC が使用される順序。 順序を指定するには、表示されている範囲内の整数を入力します。
[デフォルト VLAN（Default VLAN）] フィールド	この vNIC にデフォルトの VLAN がない場合、[なし（NONE）] をクリックします。それ以外の場合は、2 つ目のオプション ボタンをクリックし、フィールドに 1 ～ 4094 の VLAN ID を入力します。 （注） このオプションは VNTAG モードでは使用できません。
[VLAN モード（VLAN Mode）] ドロップダウン リスト	VLAN トランキングを使用する場合は、[トランク（TRUNK）] を選択します。それ以外の場合は [アクセス（ACCESS）] を選択します。 （注） このオプションは VNTAG モードでは使用できません。
[レート制限（Rate Limit）] フィールド	この vNIC に無制限のデータ レートを設定するには、[オフ（OFF）] を選択します。それ以外の場合は、2 つ目のオプション ボタンをクリックし、関連フィールドにレート制限を入力します。 1 ～ 10,000 Mbps の整数を入力します。 VIC 13xx コントローラの場合は、1 ～ 40,000 Mbps の整数を入力できます。 （注） このオプションは VNTAG モードでは使用できません。
[PXE ブートの有効化（Enable PXE Boot）] チェックボックス	vNIC を使用して PXE ブートを実行する場合は、このチェックボックスをオンにします。

名称	説明
[チャネル番号（Channel Number）] フィールド	この vNIC に割り当てるチャネル番号を選択します。 （注） このオプションには VNTAG モードが必要です。
[PCI リンク（PCI Link）] フィールド	vNIC を接続できるリンク。値は次のとおりです。 • [0]：vNIC が配置されている最初の cross-edged リンク。 • [1]：vNIC が配置されている 2 番目の cross-edged リンク。 （注） • 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 サーバだけです。
[ポート プロファイル（Port Profile）] ドロップダウン リスト	vNIC に関連付けられているポート プロファイルを選択します。 このフィールドには、このサーバが接続しているスイッチに定義されたポート プロファイルが表示されます。 （注） このオプションには VNTAG モードが必要です。
[アップリンク フェールオーバーの有効化（Enable Uplink Failover）] チェックボックス	通信の問題が発生した場合に、この vNIC 上のトラフィックをセカンダリ インターフェイスにフェールオーバーするには、このチェックボックスをオンにします。 （注） このオプションには VNTAG モードが必要です。
[VMQ の有効化（Enable VMQ）] チェックボックス	仮想マシン キュー（VMQ）を有効にするには、このチェックボックスをオンにします。 （注） SR-IOV または NetFlow オプションがアダプタで有効になっている場合に、VMQ が有効になっていないことを確認します。 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 サーバだけです。
[aRFS の有効化（Enable aRFS）] チェックボックス	Accelerated Receive Flow ステアリング（aRFS）を有効にするには、このチェックボックスをオンにします。 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 サーバだけです。

名称	説明
[NVGRE の有効化（Enable NVGRE）] チェックボックス	Generic Routing Encapsulation を使用してネットワーク仮想化を有効にするには、このチェックボックスをオンにします。 • 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 サーバだけです。 • このオプションは、Cisco VIC 1385 カードを搭載した C シリーズ サーバでのみ使用できます。
[VXLAN の有効化（Enable VXLAN）] チェックボックス	仮想拡張LANを有効にするには、このチェックボックスをオンにします。 • 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 サーバだけです。 • このオプションは、Cisco VIC 1385 カードを搭載した C シリーズ サーバでのみ使用できます。
[高度なフィルタ（Advanced Filter）] チェックボックス	vNIC で高度なフィルタ オプションを有効にするには、このチェックボックスをオンにします。
[フェールバックのタイムアウト（Failback Timeout）] フィールド	セカンダリ インターフェイスを使用して vNIC が始動した後、その vNIC のプライマリ インターフェイスが再びシステムで使用されるようにするには、プライマリ インターフェイスが一定時間使用可能な状態になっている必要があり、その時間の長さをこの設定で制御します。 0 ～ 600 の範囲の秒数を入力します。 （注） このオプションには VNTAG モードが必要です。

ステップ 5 [イーサネット割り込み（Ethernet Interrupt）] 領域で、次のフィールドの情報を確認します。

[名前（Name）]	説明
[割り込み数（Interrupt Count）] フィールド	割り当てる割り込みリソースの数。通常、この値は、完了キューリソースの数と同じにします。 1 ～ 514 の整数を入力します。
[調停タイマー（Coalescing Time）] フィールド	割り込み間の待機時間、または割り込みが送信される前に必要な休止期間。 1 ～ 65535 の整数を入力します。割り込み調停をオフにするには、このフィールドに 0（ゼロ）を入力します。

[名前（Name）]	説明
[調停タイプ（Coalescing Type）] ドロップダウン リスト	次のいずれかになります。 • [最小（MIN）]：システムは、別の割り込みイベントを送信する前に [調停時間（Coalescing Time）] フィールドに指定された時間だけ待機します。 • [アイドル（IDLE）]：アクティビティなしの期間が少なくとも [調停時間（Coalescing Time）] フィールドに指定された時間続くまで、システムから割り込みは送信されません。
[割り込みモードの選択（Interrupt Mode）] ドロップダウン リスト	優先ドライバ割り込みモード。次のいずれかになります。 • [MSI-X]：機能拡張された Message Signaled Interrupts（MSI）。これは推奨オプションです。 • [MSI]：MSI のみ。 • [INTx]：PCI INTx 割り込み。

ステップ 6 [イーサネット受信キュー（Ethernet Receive Queue）] 領域で、次のフィールドの情報を確認します。

[名前（Name）]	説明
[受信キュー数（Receive Queue Count）] フィールド	割り当てる受信キュー リソースの数。 1 ～ 256 の整数を入力します。
[受信キュー リング サイズ（Receive Queue Ring Size）] フィールド	各受信キュー内の記述子の数。 64 ～ 4096 の整数を入力します。

ステップ 7 [イーサネット送信キュー（Ethernet Transmit Queue）] 領域で、次のフィールドの情報を確認します。

[名前（Name）]	説明
[送信キュー数（Transmit Queue Count）] フィールド	割り当てる送信キュー リソースの数。 1 ～ 256 の整数を入力します。
[送信キュー リング サイズ（Transmit Queue Ring Size）] フィールド	各送信キュー内の記述子の数。 64 ～ 4096 の整数を入力します。

ステップ 8 [完了キュー（Completion Queue）] 領域で、次のフィールドの情報を確認します。

[名前（Name）]	説明
[完了キュー数（Completion Queue Count）] フィールド	割り当てる完了キューリソースの数。通常、割り当てなければならない完了キューリソースの数は、送信キューリソースの数に受信キュー リソースの数を加えたものと等しくなります。 1 ～ 512 の整数を入力します。
[完了キュー リング サイズ（Completion Queue Ring Size）] フィールド	各完了キュー内の記述子の数。 この値は変更できません。

ステップ 9 [TCP オフロード（TCP Offload）] 領域で、次のフィールドの情報を確認します。

[名前（Name）]	説明
[TCP セグメント化オフロードの有効化（Enable TCP Segmentation Offload）] チェックボックス	オンにすると、CPU はセグメント化する必要がある大きな TCP パケットをハードウェアに送信します。このオプションにより、CPU のオーバーヘッドが削減され、スループット率が向上する可能性があります。 オフにすると、CPU は大きいパケットをセグメント化します。 （注） このオプションは、Large Send Offload（LSO）とも呼ばれています。
[TCP Rx オフロードチェックサム検証の有効化（Enable TCP Rx Offload Checksum Validation）] チェックボックス	オンにすると、CPU はすべてのパケットチェックサムを検証のためにハードウェアに送信します。このオプションにより、CPU のオーバーヘッドが削減される可能性があります。 オフにすると、CPU はすべてのパケットチェックサムを検証します。
[TCP Tx オフロードチェックサム生成の有効化（Enable TCP Tx Offload Checksum Generation）] チェックボックス	オンにすると、CPU はすべてのパケットをハードウェアに送信し、ハードウェアでチェックサムを計算できるようにします。このオプションにより、CPU のオーバーヘッドが削減される可能性があります。 オフにすると、CPU はすべてのパケットチェックサムを計算します。

[名前（Name）]	説明
[大規模受信の有効化（Enable Large Receive）] チェックボックス	オンにすると、ハードウェアはすべてのセグメント化されたパケットをCPUに送信する前に再構成します。このオプションにより、CPUの使用率が削減され、インバウンドのスループットが増加する可能性があります。 オフにすると、CPU は大きいパケットをすべて処理します。

ステップ 10 [Receive Side Scaling] 領域で、次のフィールドの情報を確認します。

[名前（Name）]	説明
[TCP Receive Side Scaling の有効化（Enable TCP Receive Side Scaling）] チェックボックス	Receive Side Scaling（RSS）は、ネットワーク受信処理をマルチプロセッサ システム内の複数の CPU に分散させます。 オンにすると、可能な場合はネットワーク受信処理がプロセッサ間で共有されます。 オフにすると、ネットワーク受信処理は、追加のプロセッサが使用可能であっても、常に 1 つのプロセッサで処理されます。
[IPv4 RSS の有効化（Enable IPv4 RSS）] チェックボックス	オンにすると、RSS が IPv4 ネットワークでイネーブルになります。
[TCP-IPv4 RSS の有効化（Enable TCP-IPv4 RSS）] チェックボックス	オンにすると、IPv4 ネットワーク間の TCP 送信に対して RSS がイネーブルになります。
[IPv6 RSS の有効化（Enable IPv6 RSS）] チェックボックス	オンにすると、RSS が IPv6 ネットワークでイネーブルになります。
[TCP-IPv6 RSS の有効化（Enable TCP-IPv6 RSS）] チェックボックス	オンにすると、IPv6 ネットワーク間の TCP 送信に対して RSS がイネーブルになります。
[IPv6 拡張 RSS の有効化（Enable IPv6 Extension RSS）] チェックボックス	オンにすると、IPv6 拡張に対して RSS がイネーブルになります。
[TCP-IPv6 拡張 RSS の有効化（Enable TCP-IPv6 Extension RSS）] チェックボックス	オンにすると、IPv6 ネットワーク間の TCP 送信に対して RSS がイネーブルになります。

vNIC のプロパティの変更

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ネットワーキング（Networking）] メニューをクリックします。

ステップ 2 [アダプタ カード（Adapter Card）] ペインの [vNICs] タブをクリックします。

ステップ 3 [vNICs] ペインの [eth0] または [eth1] をクリックします。

ステップ 4 [イーサネット インターフェイス（Ethernet Interfaces）] ペインの [vNIC プロパティ（vNIC Properties）] 領域で、次のフィールドを更新します。

[名前（Name）]	説明
[名前（Name）] フィールド	仮想 NIC の名前。 この名前は、vNIC の作成後は変更できません。
[CDN] フィールド	VIC カードのイーサネット vNIC に割り当てることができる一貫したデバイス名（CDN）。特定の CDN をデバイスに割り当てることで、ホスト OS 上でそれを識別できます。 （注） この機能は、[VIC に対する CDN サポート（CDN Support for VIC）] トークンが BIOS で有効になっている場合にのみ機能します。
[MTU] フィールド	この vNIC で受け入れられる最大伝送単位、つまりパケット サイズ。 1500 ～ 9000 の整数を入力します。
[アップリンク ポート（Uplink Port）] ドロップダウン リスト	この vNIC に関連付けられたアップリンク ポート。この vNIC に対するすべてのトラフィックは、このアップリンク ポートを通過します。
[MACアドレス（MAC Address）] フィールド	vNIC に関連付けられた MAC アドレス。 アダプタが内部プールから使用可能な MAC アドレスを選択するようにするには、[自動（Auto）] を選択します。アドレスを指定するには、2 番目のオプション ボタンをクリックし、対応するフィールドに MAC アドレスを入力します。

[名前（Name）]	説明
[サービス クラス（Class of Service）] ドロップダウン リスト	この vNIC からのトラフィックに関連付けられるサービス クラス。 0 ～ 6 の整数を選択します。0 が最も低い優先度で、6 が最も高い優先度になります。 （注） このオプションは VNTAG モードでは使用できません。
[信頼ホスト CoS（Trust Host CoS）] チェックボックス	vNIC で、ホスト オペレーティング システムが提供するサービス クラスを使用できるようにするには、このチェックボックスをオンにします。
[PCI リンク（PCI Link）] フィールド	vNIC を接続できるリンク。値は次のとおりです。 • [0]：vNIC が配置されている最初の cross-edged リンク。 • [1]：vNIC が配置されている 2 番目の cross-edged リンク。 （注） • 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 サーバだけです。 • このオプションは、Cisco VIC 1385 カードを搭載した C シリーズ サーバでのみ使用できます。
[PCI 順序（PCI Order）] フィールド	この vNIC が使用される順序。 システムが順序を設定するようにするには、[いずれか（Any）] を選択します。順序を指定する場合、2 つ目のオプション ボタンを選択し、0 ～ 17 の整数を入力します。
[デフォルト VLAN（Default VLAN）] フィールド	この vNIC にデフォルトの VLAN がない場合、[なし（NONE）] をクリックします。それ以外の場合は、2 つ目のオプション ボタンをクリックし、フィールドに 1 ～ 4094 の VLAN ID を入力します。 （注） このオプションは VNTAG モードでは使用できません。

[名前（Name）]	説明
[VLAN モード（VLAN Mode）] ドロップダウン リスト	VLAN トランキングを使用する場合は、[トランク（TRUNK）] を選択します。それ以外の場合は [アクセス（ACCESS）] を選択します。VLAN が [アクセス（ACCESS）] モードに設定されている場合、TAG付きのスイッチから受信されており、さらに指定されたデフォルトの VLAN（1-4094）から受信されているフレームは、vNIC 経由でホスト OS に送信されると、その TAG を削除します。 （注） このオプションは VNTAG モードでは使用できません。
[レート制限（Rate Limit）] フィールド	この vNIC に無制限のデータ レートを設定するには、[オフ（OFF）] を選択します。それ以外の場合は、2 つ目のオプション ボタンをクリックし、関連フィールドにレート制限を入力します。 選択したアダプタ カードに応じて、1 ～ 10,000 Mbps または 40,000 Mbps の間の整数を入力します。 （注） このオプションは VNTAG モードでは使用できません。
[PXE ブートの有効化（Enable PXE Boot）] チェックボックス	vNIC を使用して PXE ブートを実行する場合は、このチェックボックスをオンにします。
[チャネル番号（Channel Number）] フィールド	この vNIC に割り当てるチャネル番号を選択します。 （注） このオプションには VNTAG モードが必要です。
[ポート プロファイル（Port Profile）] ドロップダウン リスト	vNIC に関連付けられているポート プロファイルを選択します。 このフィールドには、このサーバが接続しているスイッチに定義されたポート プロファイルが表示されます。 （注） このオプションには VNTAG モードが必要です。
[アップリンク フェールオーバーの有効化（Enable Uplink Failover）] チェックボックス	通信の問題が発生した場合に、この vNIC 上のトラフィックをセカンダリ インターフェイスにフェールオーバーするには、このチェックボックスをオンにします。 （注） このオプションには VNTAG モードが必要です。

[名前（Name）]	説明
[VMQ の有効化（Enable VMQ）] チェックボックス	仮想マシン キュー（VMQ）を有効にするには、このチェックボックスをオンにします。 （注） SR-IOV または NetFlow オプションがアダプタで有効になっている場合に、VMQ が有効になっていないことを確認します。 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 サーバだけです。
[aRFS の有効化（Enable aRFS）] チェックボックス	Accelerated Receive Flow ステアリング（aRFS）を有効にするには、このチェックボックスをオンにします。 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 サーバだけです。
[NVGRE の有効化（Enable NVGRE）] チェックボックス	Generic Routing Encapsulation を使用してネットワーク仮想化を有効にするには、このチェックボックスをオンにします。 • 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 サーバだけです。 • このオプションは、Cisco VIC 1385 カードを搭載した C シリーズ サーバでのみ使用できます。
[VXLAN の有効化（Enable VXLAN）] チェックボックス	仮想拡張LANを有効にするには、このチェックボックスをオンにします。 • 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 サーバだけです。 • このオプションは、Cisco VIC 1385 カードを搭載した C シリーズ サーバでのみ使用できます。
[フェールバックのタイムアウト（Failback Timeout）] フィールド	セカンダリ インターフェイスを使用して vNIC が始動した後、その vNIC のプライマリ インターフェイスが再びシステムで使用されるようにするには、プライマリ インターフェイスが一定時間使用可能な状態になっている必要があり、その時間の長さをこの設定で制御します。 0 ～ 600 の範囲の秒数を入力します。 （注） このオプションには VNTAG モードが必要です。

ステップ 5 [イーサネット割り込み（Ethernet Interrupt）] 領域で、次のフィールドを更新します。

[名前（Name）]	説明
[割り込み数（Interrupt Count）] フィールド	割り当てる割り込みリソースの数。通常、この値は、完了キューリソースの数と同じにします。 1 ～ 514 の整数を入力します。
[調停タイマー（Coalescing Time）] フィールド	割り込み間の待機時間、または割り込みが送信される前に必要な休止期間。 1 ～ 65535 の整数を入力します。割り込み調停をオフにするには、このフィールドに 0（ゼロ）を入力します。
[調停タイプ（Coalescing Type）] ドロップダウン リスト	次のいずれかになります。 • [最小（MIN）]：システムは、別の割り込みイベントを送信する前に [調停時間（Coalescing Time）] フィールドに指定された時間だけ待機します。 • [アイドル（IDLE）]：アクティビティなしの期間が少なくとも [調停時間（Coalescing Time）] フィールドに指定された時間続くまで、システムから割り込みは送信されません。
[割り込みモードの選択（Interrupt Mode）] ドロップダウン リスト	優先ドライバ割り込みモード。次のいずれかになります。 • [MSI-X]：機能拡張された Message Signaled Interrupts（MSI）。これは推奨オプションです。 • [MSI]：MSI のみ。 • [INTx]：PCI INTx 割り込み。

ステップ 6 [イーサネット受信キュー（Ethernet Receive Queue）] 領域で、次のフィールドを更新します。

[名前（Name）]	説明
[受信キュー数（Receive Queue Count）] フィールド	割り当てる受信キュー リソースの数。 1 ～ 256 の整数を入力します。
[受信キュー リング サイズ（Receive Queue Ring Size）] フィールド	各受信キュー内の記述子の数。 64 ～ 4096 の整数を入力します。

ステップ 7 [イーサネット送信キュー（Ethernet Transmit Queue）] 領域で、次のフィールドを更新します。

[名前（Name）]	説明
[送信キュー数（Transmit Queue Count）] フィールド	割り当てる送信キュー リソースの数。 1 ～ 256 の整数を入力します。
[送信キュー リング サイズ（Transmit Queue Ring Size）] フィールド	各送信キュー内の記述子の数。 64 ～ 4096 の整数を入力します。

ステップ 8 [完了キュー（Completion Queue）] 領域で、次のフィールドを更新します。

[名前（Name）]	説明
[完了キュー数（Completion Queue Count）] フィールド	割り当てる完了キュー リソースの数。通常、割り当てなければならない完了キュー リソースの数は、送信キュー リソースの数に受信キュー リソースの数を加えたものと等しくなります。 1 ～ 512 の整数を入力します。
[完了キュー リング サイズ（Completion Queue Ring Size）] フィールド	各完了キュー内の記述子の数。 この値は変更できません。

ステップ 9 [TCP オフロード（TCP Offload）] 領域で、次のフィールドを更新します。

[名前（Name）]	説明
[TCP セグメント化オフロードの有効化（Enable TCP Segmentation Offload）] チェックボックス	オンにすると、CPU はセグメント化する必要がある大きな TCP パケットをハードウェアに送信します。このオプションにより、CPU のオーバーヘッドが削減され、スループット率が向上する可能性があります。 オフにすると、CPU は大きいパケットをセグメント化します。 （注） このオプションは、Large Send Offload（LSO）とも呼ばれています。
[TCP Rx オフロード チェックサム検証の有効化（Enable TCP Rx Offload Checksum Validation）] チェックボックス	オンにすると、CPU はすべてのパケット チェックサムを検証のためにハードウェアに送信します。このオプションにより、CPU のオーバーヘッドが削減される可能性があります。 オフにすると、CPU はすべてのパケット チェックサムを検証します。

[名前（Name）]	説明
[TCP Tx オフロードチェックサム生成の有効化（Enable TCP Tx Offload Checksum Generation）] チェックボックス	オンにすると、CPU はすべてのパケットをハードウェアに送信し、ハードウェアでチェックサムを計算できるようにします。このオプションにより、CPU のオーバーヘッドが削減される可能性があります。 オフにすると、CPU はすべてのパケットチェックサムを計算します。
[大規模受信の有効化（Enable Large Receive）] チェックボックス	オンにすると、ハードウェアはすべてのセグメント化されたパケットを CPU に送信する前に再構成します。このオプションにより、CPU の使用率が削減され、インバウンドのスループットが増加する可能性があります。 オフにすると、CPU は大きいパケットをすべて処理します。

ステップ 10 [Receive Side Scaling] 領域で、次のフィールドを更新します。

[名前（Name）]	説明
[TCP Receive Side Scaling の有効化（Enable TCP Receive Side Scaling）] チェックボックス	Receive Side Scaling（RSS）は、ネットワーク受信処理をマルチプロセッサ システム内の複数の CPU に分散させます。 オンにすると、可能な場合はネットワーク受信処理がプロセッサ間で共有されます。 オフにすると、ネットワーク受信処理は、追加のプロセッサが使用可能であっても、常に 1 つのプロセッサで処理されます。
[IPv4 RSS の有効化（Enable IPv4 RSS）] チェックボックス	オンにすると、RSS が IPv4 ネットワークでイネーブルになります。
[TCP-IPv4 RSS の有効化（Enable TCP-IPv4 RSS）] チェックボックス	オンにすると、IPv4 ネットワーク間の TCP 送信に対して RSS がイネーブルになります。
[IPv6 RSS の有効化（Enable IPv6 RSS）] チェックボックス	オンにすると、RSS が IPv6 ネットワークでイネーブルになります。
[TCP-IPv6 RSS の有効化（Enable TCP-IPv6 RSS）] チェックボックス	オンにすると、IPv6 ネットワーク間の TCP 送信に対して RSS がイネーブルになります。
[IPv6 拡張 RSS の有効化（Enable IPv6 Extension RSS）] チェックボックス	オンにすると、IPv6 拡張に対して RSS がイネーブルになります。

[名前（Name）]	説明
[TCP-IPv6 拡張 RSS の有効化（Enable TCP-IPv6 Extension RSS）] チェックボックス	オンにすると、IPv6 ネットワーク間の TCP 送信に対して RSS がイネーブルになります。

ステップ 11 [変更の保存（Save Changes）] をクリックします。

vNIC の作成

アダプタは、永続的な vNIC を 2 つ提供します。追加の vNIC を 16 個まで作成できます。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ネットワーキング（Networking）] メニューをクリックします。

ステップ 2 [アダプタ カード（Adapter Card）] ペインの [vNICs] タブをクリックします。

ステップ 3 [ホスト イーサネット インターフェイス（Host Ethernet Interfaces）] 領域で、次のアクションのいずれかを選択します。

- デフォルトの設定を使用して vNIC を作成するには、[vNIC の追加（Add vNIC）] をクリックします。
- 既存の vNIC と同じ設定を使用して vNIC を作成するには、その vNIC を選択し、[vNIC の複製（Clone vNIC）] をクリックします。

[vNIC の追加（Add vNIC）] ダイアログボックスが表示されます。

ステップ 4 [vNIC の追加（Add vNIC）] ダイアログボックスで、vNIC の名前を 名前 入力ボックスに入力します。

ステップ 5 （任意） [vNIC の追加（Add vNIC）] ダイアログボックスで、vNIC のチャネル番号を [チャネル番号（Channel Number）] 入力ボックスに入力します。

（注） アダプタで NIV がイネーブルになっている場合、vNIC を作成するときに vNIC のチャネル番号を割り当てる必要があります。

ステップ 6 [vNIC の追加（Add vNIC）] をクリックします。

次の作業

設定の変更が必要な場合は、vNIC のプロパティの変更, （221 ページ） の説明に従って、新しい vNIC を設定します。

vNIC の削除

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ネットワーキング（Networking）] メニューをクリックします。

ステップ 2 [アダプタ カード（Adapter Card）] ペインの [vNICs] タブをクリックします。

ステップ 3 [ホスト イーサネット インターフェイス（Host Ethernet Interfaces）] 領域で、表から vNIC を選択します。

（注） デフォルトの 2 つの vNIC（[eth0] と [eth1]）は、どちらも削除することはできません。

ステップ 4 [vNIC の削除（Delete vNIC）] をクリックし、[OK] をクリックして確認します。

Cisco usNIC の管理

Cisco usNIC の概要

Cisco user-space NIC（Cisco usNIC）機能は、ネットワーキング パケットの送受信時にカーネルをバイパスすることにより、データセンターの Cisco UCS サーバで稼動しているソフトウェア アプリケーションのパフォーマンスを向上させます。アプリケーションは などの Cisco UCS VIC 第 2 世代以降のアダプタと直接やり取りするので、ハイ パフォーマンス コンピューティング クラスタのネットワーキング パフォーマンスが向上します。Cisco usNIC のメリットを享受するには、ソケットやその他の通信 API ではなく、Message Passing Interface（MPI）をアプリケーションで使用する必要があります。

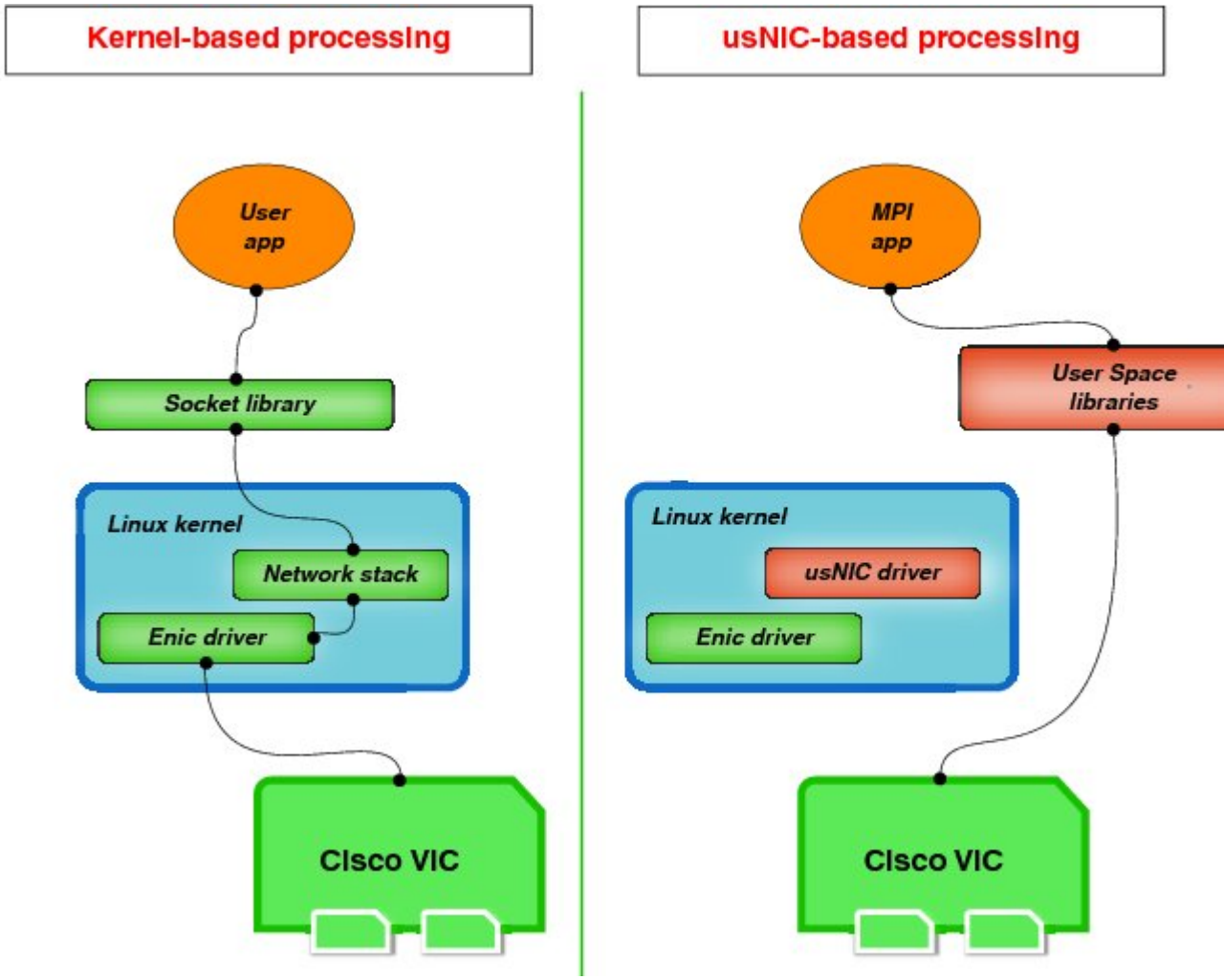
Cisco usNIC を使用すると、MPI アプリケーションで次の利点が得られます。

- 低遅延で、高スループットの通信転送を提供します。
- 標準のアプリケーション非依存イーサネット プロトコルを実行します。
- 次に示すシスコ データセンター プラットフォームで、低遅延の転送、ユニファイド ファブリック、統合管理のサポートを活用します。
  - Cisco UCS サーバ
  - 第二世代以降の Cisco UCS VIC アダプタ
  - 10 または 40GbE ネットワーク

標準イーサネット アプリケーションは、Linux カーネルのネットワーキング スタックを呼び出すユーザ領域のソケット ライブラリを使用します。次に、ネットワーキング スタックは Cisco eNIC

ドライバを使用して、Cisco VIC ハードウェアと通信します。次の図は、通常のソフトウェア アプリケーションと Cisco usNIC を使用する MPI アプリケーションの対比を示しています。

図 *1*：カーネル ベースのネットワーク通信と *Cisco usNIC* ベースの通信



Cisco IMC GUI を使用した Cisco usNIC の表示および設定

はじめる前に

このタスクを実行するには、管理者権限で Cisco IMC GUI にログインする必要があります。このビデオの [再生（Play）] をクリックして、CIMC で Cisco usNIC を設定する方法を視聴します。

手順

ステップ 1 Cisco IMC GUI にログインします。

Cisco IMC へのログイン方法に関する詳細については、『Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide』を参照してください。

ステップ 2 [ナビゲーション（Navigation）] ペインの [ネットワーキング（Networking）] メニューをクリックします。

ステップ 3 [アダプタ カード（Adapter Card）] ペインの [vNICs] タブをクリックします。

ステップ 4 [vNICs] ペインの [eth0] または [eth1] をクリックします。

ステップ 5 [イーサネット インターフェイス（Ethernet Interfaces）] 領域で、[usNIC] 領域を選択します。

ステップ 6 [プロパティ（Properties）] 領域で、次のフィールドを確認して更新します。

[名前（Name）]	説明
[名前（Name）]	usNIC の親である vNIC の名前。 （注） このフィールドは読み取り専用です。
[usNIC] フィールド	特定の vNIC に割り当てられる usNIC の数。 0 ～ 225 の整数を入力します。 指定の vNIC に追加の usNIC を割り当てるには、既存の値よりも高い値を入力してください。 指定の vNIC から usNIC を削除するには、既存の値よりも小さい値を入力します。 vNIC に割り当てられたすべての usNIC を削除するには、ゼロを入力します。
[送信キュー数（Transmit Queue Count）] フィールド	割り当てる送信キュー リソースの数。 1 ～ 256 の整数を入力します。
[受信キュー数（Receive Queue Count）] フィールド	割り当てる受信キュー リソースの数。 1 ～ 256 の整数を入力します。
[完了キュー数（Completion Queue Count）] フィールド	割り当てる完了キュー リソースの数。通常、割り当てなければならない完了キュー リソースの数は、送信キュー リソースの数に受信キュー リソースの数を加えたものと等しくなります。 1 ～ 512 の整数を入力します。
[送信キュー リング サイズ（Transmit Queue Ring Size）] フィールド	各送信キュー内の記述子の数。 64 ～ 4096 の整数を入力します。
[受信キュー リング サイズ（Receive Queue Ring Size）] フィールド	各受信キュー内の記述子の数。 64 ～ 4096 の整数を入力します。

[名前（Name）]	説明
[割り込み数（Interrupt Count）] フィールド	割り当てる割り込みリソースの数。通常、この値は、完了キュー リソースの数と同じにします。 1 ～ 514 の整数を入力します。
[割り込み調停タイプ（Interrupt Coalescing Type）] ドロップダウン リスト	次のいずれかになります。 • [最小（MIN）] : システムは、別の割り込みイベントを送信する前に [調停時間（Coalescing Time）] フィールドに指定された時間だけ待機します。 • [アイドル（IDLE）] : アクティビティなしの期間が少なくとも [調停時間（Coalescing Time）] フィールドに指定された時間続くまで、システムから割り込みは送信されません。
[割り込み調停タイマー時間（Interrupt Coalescing Timer Time）] フィールド	割り込み間の待機時間、または割り込みが送信される前に必要な休止期間。 1 ～ 65535 の整数を入力します。割り込み調停をオフにするには、このフィールドに0（ゼロ）を入力します。
[サービス クラス（Class of Service）] フィールド	この usNIC からのトラフィックに関連付けられるサービス クラス。 0 ～ 6 の整数を選択します。0 が最も低い優先度で、6 が最も高い優先度になります。 （注） このオプションは VNTAG モードでは使用できません。
[TCP セグメント オフロード（TCP Segment Offload）] チェックボックス	オンにすると、CPU はセグメント化する必要がある大きな TCP パケットをハードウェアに送信します。このオプションにより、CPU のオーバーヘッドが削減され、スループット率が向上する可能性があります。 オフにすると、CPU は大きいパケットをセグメント化します。 （注） このオプションは、Large Send Offload（LSO）とも呼ばれています。

[名前（Name）]	説明
[大規模受信（Large Receive）] チェックボックス	オンにすると、ハードウェアはすべてのセグメント化されたパケットを CPU に送信する前に再構成します。このオプションにより、CPU の使用率が削減され、インバウンドのスループットが増加する可能性があります。 オフにすると、CPU は大きいパケットをすべて処理します。
[TCP Tx チェックサム（TCP Tx Checksum）] チェックボックス	オンにすると、CPU はすべてのパケットをハードウェアに送信し、ハードウェアでチェックサムを計算できるようにします。このオプションにより、CPU のオーバーヘッドが削減される可能性があります。 オフにすると、CPU はすべてのパケット チェックサムを計算します。
[TCP Rx チェックサム（TCP Rx Checksum）] チェックボックス	オンにすると、CPU はすべてのパケット チェックサムを検証のためにハードウェアに送信します。このオプションにより、CPU のオーバーヘッドが削減される可能性があります。 オフにすると、CPU はすべてのパケット チェックサムを検証します。

ステップ 7 [変更の保存（Save Changes）] をクリックします。
変更内容は次のサーバのリブート時に有効になります。

usNIC プロパティの表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ネットワーキング（Networking）] メニューをクリックします。

ステップ 2 [アダプタ カード（Adapter Card）] ペインの [vNICs] タブをクリックします。

ステップ 3 [vNICs] ペインの [eth0] または [eth1] をクリックします。

ステップ 4 [ホスト イーサネット インターフェイス（Host Ethernet Interfaces）] ペインの [usNIC プロパティ（usNIC Properties）] 領域で、次のフィールドの情報を確認します。

[名前（Name）]	説明
[名前（Name）]	usNIC の親である vNIC の名前。 （注） このフィールドは読み取り専用です。
[usNIC] フィールド	特定の vNIC に割り当てられる usNIC の数。 0 ～ 225 の整数を入力します。 指定の vNIC に追加の usNIC を割り当てるには、既存の値よりも高い値を入力してください。 指定の vNIC から usNIC を削除するには、既存の値よりも小さい値を入力します。 vNIC に割り当てられたすべての usNIC を削除するには、ゼロを入力します。
[送信キュー数（Transmit Queue Count）] フィールド	割り当てる送信キュー リソースの数。 1 ～ 256 の整数を入力します。
[受信キュー数（Receive Queue Count）] フィールド	割り当てる受信キュー リソースの数。 1 ～ 256 の整数を入力します。
[完了キュー数（Completion Queue Count）] フィールド	割り当てる完了キューリソースの数。通常、割り当てなければならない完了キューリソースの数は、送信キュー リソースの数に受信キュー リソースの数を加えたものと等しくなります。 1 ～ 512 の整数を入力します。
[送信キュー リング サイズ（Transmit Queue Ring Size）] フィールド	各送信キュー内の記述子の数。 64 ～ 4096 の整数を入力します。
[受信キュー リング サイズ（Receive Queue Ring Size）] フィールド	各受信キュー内の記述子の数。 64 ～ 4096 の整数を入力します。
[割り込み数（Interrupt Count）] フィールド	割り当てる割り込みリソースの数。通常、この値は、完了キュー リソースの数と同じにします。 1 ～ 514 の整数を入力します。

[名前（Name）]	説明
[割り込み調停タイプ（Interrupt Coalescing Type）] ドロップダウン リスト	次のいずれかになります。 • [最小（MIN）]：システムは、別の割り込みイベントを送信する前に [調停時間（Coalescing Time）] フィールドに指定された時間だけ待機します。 • [アイドル（IDLE）]：アクティビティなしの期間が少なくとも [調停時間（Coalescing Time）] フィールドに指定された時間続くまで、システムから割り込みは送信されません。
[割り込み調停タイマー時間（Interrupt Coalescing Timer Time）] フィールド	割り込み間の待機時間、または割り込みが送信される前に必要な休止期間。 1 ～ 65535 の整数を入力します。割り込み調停をオフにするには、このフィールドに0（ゼロ）を入力します。
[サービス クラス（Class of Service）] フィールド	このusNICからのトラフィックに関連付けられるサービス クラス。 0 ～ 6 の整数を選択します。0 が最も低い優先度で、6 が最も高い優先度になります。 （注） このオプションは VNTAG モードでは使用できません。
[TCP セグメント オフロード（TCP Segment Offload）] チェックボックス	オンにすると、CPUはセグメント化する必要がある大きなTCPパケットをハードウェアに送信します。このオプションにより、CPU のオーバーヘッドが削減され、スループット率が向上する可能性があります。 オフにすると、CPUは大きいパケットをセグメント化します。 （注） このオプションは、Large Send Offload（LSO）とも呼ばれています。

[名前（Name）]	説明
[大規模受信（Large Receive）] チェックボックス	オンにすると、ハードウェアはすべてのセグメント化されたパケットを CPU に送信する前に再構成します。このオプションにより、CPU の使用率が削減され、インバウンドのスループットが増加する可能性があります。 オフにすると、CPU は大きいパケットをすべて処理します。
[TCP Tx チェックサム（TCP Tx Checksum）] チェックボックス	オンにすると、CPU はすべてのパケットをハードウェアに送信し、ハードウェアでチェックサムを計算できるようにします。このオプションにより、CPU のオーバーヘッドが削減される可能性があります。 オフにすると、CPU はすべてのパケットチェックサムを計算します。
[TCP Rx チェックサム（TCP Rx Checksum）] チェックボックス	オンにすると、CPU はすべてのパケットチェックサムを検証のためにハードウェアに送信します。このオプションにより、CPU のオーバーヘッドが削減される可能性があります。 オフにすると、CPU はすべてのパケットチェックサムを検証します。

iSCSI ブート機能の設定

vNIC の iSCSI ブート機能の設定

ラック サーバがスタンドアロン モードに設定されていて、VIC アダプタが Nexus 5000 および Nexus 6000 スイッチ ファミリに直接接続されている場合は、iSCSI ストレージ ターゲットからサーバがリモートでブートされるようにこれらの VIC アダプタを設定できます。ラック サーバがリモート iSCSI ターゲット デバイスからホスト OS イメージをロードできるようにイーサネット vNIC を設定できます。

vNIC で iSCSI ブート機能を設定する方法は、次のとおりです。

- このタスクを実行するには、admin 権限でログインする必要があります。

- iSCSI ストレージ ターゲットからサーバをリモートでブートするように vNIC を設定するには、vNIC の PXE ブート オプションをイネーブルにする必要があります。

（注） ホストごとに最大 2 つの iSCSI vNIC を設定できます。

vNIC 上の iSCSI ブート機能の設定

ホストごとに最大 2 つの iSCSI vNIC を設定できます。

はじめる前に

- iSCSI ストレージ ターゲットからサーバをリモートでブートするように vNIC を設定するには、vNIC の PXE ブート オプションをイネーブルにする必要があります。
- このタスクを実行するには、admin 権限で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 [ネットワーキング（Networking）] メニューをクリックします。

ステップ 2 [アダプタ カード（Adapter Card）] ペインの [vNICs] タブをクリックします。

ステップ 3 [vNICs] ペインの [eth0] または [eth1] をクリックします。

ステップ 4 [イーサネット インターフェイス（Ethernet Interfaces）] 領域で、[iSCSI ブート プロパティ（iSCSI Boot Properties）] 領域を選択します。

ステップ 5 [全般（General）] 領域で、次のフィールドを更新します。

[名前（Name）]	説明
[名前（Name）] フィールド	vNIC の名前。
[DHCP ネットワーク（DHCP Network）] チェックボックス	vNIC に対して DHCP ネットワークがイネーブルかどうか。 イネーブルの場合、イニシエータのネットワーク設定を DHCP サーバから取得します。
[DHCP iSCSI] チェックボックス	vNIC に対して DHCP iSCSI がイネーブルかどうか。イネーブルになっていて DHCP ID が設定されている場合、イニシエータ IQN とターゲットの情報を DHCP サーバから取得します。 （注） DHCP iSCSI が DHCP ID なしでイネーブルに設定されている場合、ターゲット情報のみを取得します。

[名前（Name）]	説明
[DHCP ID] フィールド	イニシエータ IQN とターゲットの情報を DHCP サーバから取得するためにアダプタが使用するベンダー識別文字列。 最大 64 文字の文字列を入力します。
[DHCPタイムアウト（DHCP Timeout）] フィールド	イニシエータが DHCP サーバが使用できないと判断するまでに待機する秒数。 60 ～ 300 の整数を入力します（デフォルトは 60 秒です）。
[リンク タイムアウト（Link Timeout）] フィールド	リンクが使用できないとイニシエータが判断するまで待機する秒数。 0 ～ 255 の整数を入力します（デフォルトは 15 秒です）。
[LUN再試行回数値の入力（LUN Busy Retry Count）] フィールド	iSCSI LUN 検出中にエラーが発生した場合に接続を再試行する回数。 0 ～ 255 の整数を入力します。デフォルトは 15 です。
[IP バージョン（IP Version）] フィールド	iSCSI ブート中に使用する IP バージョン。

ステップ 6 [イニシエータ（Initiator）] 領域で、次のフィールドを更新します。

[名前（Name）]	説明
[名前（Name）] フィールド	iSCSI イニシエータ名を定義する正規表現。 任意の英数字および次の特殊文字を入力することができます。 • .（ピリオド） • :（コロン） • -（ダッシュ） （注） 名前は、IQN 形式です。
[IPアドレス（IP Address）] フィールド	iSCSI イニシエータの IP アドレス。
[サブネット マスク（Subnet Mask）] フィールド	iSCSI イニシエータのサブネット マスク。
[ゲートウェイ（Gateway）] フィールド	デフォルト ゲートウェイ。

[名前（Name）]	説明
[プライマリ DNS（Primary DNS）] フィールド	プライマリ DNS サーバのアドレス。
[セカンダリDNS（Secondary DNS）] フィールド	セカンダリ DNS サーバ アドレス。
[TCP タイムアウト（TCP Timeout）] フィールド	TCP が使用できないとイニシエータが判断するまで待機する秒数。 0 ～ 255 の整数を入力します（デフォルトは 15 秒です）。
[CHAP 名（CHAP Name）] フィールド	イニシエータの Challenge Handshake Authentication Protocol（CHAP）の名前。
[CHAPシークレット（CHAP Secret）] フィールド	イニシエータの Challenge Handshake Authentication Protocol（CHAP）の共有秘密。

ステップ 7 [プライマリ ターゲット（Primary Target）] 領域で、次のフィールドを更新します。

[名前（Name）]	説明
[名前（Name）] フィールド	IQN 形式のプライマリ ターゲットの名前。
[IPアドレス（IP Address）] フィールド	ターゲットの IP アドレス。
[TCP ポート（TCP Port）] フィールド	ターゲットに関連付けられた TCP ポート。
[ブート LUN（Boot LUN）] フィールド	ターゲットに関連付けられたブート LUN。
[CHAP 名（CHAP Name）] フィールド	イニシエータの Challenge Handshake Authentication Protocol（CHAP）の名前。
[CHAPシークレット（CHAP Secret）] フィールド	イニシエータの Challenge Handshake Authentication Protocol（CHAP）の共有秘密。

ステップ 8 [セカンダリ ターゲット（Secondary Target）] 領域で、次のフィールドを更新します。

[名前（Name）]	説明
[名前（Name）] フィールド	IQN 形式のセカンダリ ターゲットの名前。

[名前（Name）]	説明
[IPアドレス（IP Address）] フィールド	ターゲットの IP アドレス。
[TCP ポート（TCP Port）] フィールド	ターゲットに関連付けられた TCP ポート。
[ブート LUN（Boot LUN）] フィールド	ターゲットに関連付けられたブート LUN。
[CHAP 名（CHAP Name）] フィールド	イニシエータの Challenge Handshake Authentication Protocol（CHAP）の名前。
[CHAPシークレット（CHAP Secret）] フィールド	イニシエータの Challenge Handshake Authentication Protocol（CHAP）の共有秘密。

[名前（Name）]	説明
[ISCSI の設定（Configure ISCSI）] ボタン	選択された vNIC で iSCSI ブートを設定します。
[ISCSI の構成解除（Unconfigure ISCSI）] ボタン	選択された vNIC から設定を削除します。
[値のリセット（Reset Values）] ボタン	vNIC 用の値を、このダイアログボックスを最初に開いたときに有効になっていた設定に復元します。
[キャンセル（Cancel）] ボタン	変更を加えずにダイアログボックスを閉じます。

ステップ 9 [変更の保存（Save Changes）] をクリックします。

vNIC からの iSCSI ブート設定の除去

はじめる前に

このタスクを実行するには、admin 権限で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 [ネットワーキング（Networking）] メニューをクリックします。

ステップ 2 [アダプタ カード（Adapter Card）] ペインの [vNICs] タブをクリックします。

ステップ 3 [vNICs] ペインの [eth0] または [eth1] をクリックします。

ステップ 4 [イーサネット インターフェイス（Ethernet Interfaces）] 領域で、[iSCSI ブート プロパティ（iSCSI Boot Properties）] 領域を選択します。

ステップ 5 領域下部にある [ISCSI の構成解除（Unconfigure ISCSI）] ボタンをクリックします。

アダプタ設定のバックアップと復元

アダプタ設定のエクスポート

アダプタ設定は、次のいずれかになるリモート サーバに XML ファイルとしてエクスポートできます。

- TFTP
- FTP
- SFTP
- SCP
- HTTP

はじめる前に

リモート サーバの IP アドレスを取得します。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ネットワーキング（Networking）] メニューをクリックします。

ステップ 2 [アダプタ カード（Adapter Card）] タブをクリックします。
[全般（General）] タブが表示されます。

ステップ 3 [全般（General）] タブの [アクション（Actions）] 領域で、[エクスポート設定（Export Configuration）] をクリックします。
[アダプタ設定のエクスポート（Export Adapter Configuration）] ダイアログボックスが開きます。

ステップ 4 [アダプタ設定のエクスポート（Export Adapter Configuration）] ダイアログボックスで、次のフィールドを更新します。

名称	説明
[エクスポート先（Export to）] ドロップダウン リスト	リモート サーバのタイプ。次のいずれかになります。 • TFTP サーバ（TFTP Server） • FTP サーバ（FTP Server） • SFTP サーバ（SFTP Server） • SCP サーバ • HTTP サーバ（HTTP Server） （注） このアクションを実行しながら、リモートサーバタイプとして SCP または SFTP を選択した場合、「サーバ（*RSA*）キー 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?*）」というメッセージとともにポップアップ ウィンドウが表示されます。サーバ フィンガープリントの信頼性に応じて、[はい（Yes）] または [いいえ（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に基づいており、接続先のホストを識別または確認できます。
[サーバIP/ホスト名（Server IP/Hostname）] フィールド	アダプタ設定ファイルのエクスポート先となるサーバの IPv4 アドレスか IPv6 アドレス、またはホスト名。[エクスポート先（Export to）] 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。
[パスおよびファイル名（Path and Filename）] フィールド	ファイルをリモート サーバにエクスポートするときに、Cisco IMC で使用するパスおよびファイル名。
[ユーザ名（Username）]	システムがリモート サーバへのログインに使用する必要のあるユーザ名。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。
[パスワード（Password）]	リモート サーバのユーザ名のパスワード。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。

ステップ 5 [設定のエクスポート（Export Configuration）] をクリックします。

アダプタ設定のインポート

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ネットワーキング（Networking）] メニューをクリックします。

ステップ 2 [アダプタ カード（Adapter Card）] タブをクリックします。
[全般（General）] タブが表示されます。

ステップ 3 [全般（General）] タブの [アクション（Actions）] 領域で、[インポート設定（Import Configuration）] をクリックします。
[アダプタ設定のインポート（Import Adapter Configuration）] ダイアログボックスが開きます。

ステップ 4 [アダプタ設定のインポート（Import Adapter Configuration）] ダイアログボックスで、次のフィールドを更新します。

名称	説明
[インポート元（Import from）] ドロップダウン リスト	リモート サーバのタイプ。次のいずれかになります。 • TFTP サーバ（TFTP Server） • FTP サーバ（FTP Server） • SFTP サーバ（SFTP Server） • SCP サーバ • HTTP サーバ（HTTP Server） （注） このアクションを実行しながら、リモート サーバタイプとして SCP または SFTP を選択した場合、「サーバ（*RSA*）キー 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?*）」というメッセージとともにポップアップ ウィンドウが表示されます。サーバ フィンガープリントの信頼性に応じて、[はい（Yes）] または [いいえ（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に基づいており、接続先のホストを識別または確認できます。
[サーバIP/ホスト名（Server IP/Hostname）] フィールド	アダプタ設定ファイルが存在するサーバの IPv4 アドレスか IPv6 アドレス、またはホスト名。[インポート元（Import 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。

名称	説明
[パスおよびファイル名（Path and Filename）] フィールド	リモート サーバ上の設定ファイルのパスおよびファイル名。
[ユーザ名（Username）]	システムがリモートサーバへのログインに使用する必要のあるユーザ名。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。
[パスワード（Password）]	リモート サーバのユーザ名のパスワード。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。

ステップ 5 [設定のインポート（Import Configuration）] をクリックします。
アダプタは、指定された IP アドレスの TFTP サーバから、指定されたパスの設定ファイルをダウンロードします。この設定は、サーバが次にリブートされたときにインストールされます。

次の作業

サーバをリブートして、インポートした設定を適用します。

アダプタのデフォルトの復元

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ネットワーキング（Networking）] メニューをクリックします。

ステップ 2 [アダプタ カード（Adapter Card）] タブをクリックします。
[全般（General）] タブが表示されます。

ステップ 3 [全般（General）] タブの [アクション（Actions）] 領域で、[デフォルトにリセット（Reset To Defaults）] をクリックし、[OK] をクリックして確定します。

（注） アダプタをデフォルト設定にリセットすると、ポート速度が 4 X 10 Gbps に設定されます。40 Gbps スイッチを使用している場合にのみ、ポート速度として 40 Gbps を選択してください。

アダプタのリセット

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ネットワーキング（Networking）] メニューをクリックします。

ステップ 2 [アダプタ カード（Adapter Card）] タブをクリックします。
[全般（General）] タブが表示されます。

ステップ 3 [全般（General）] タブの [アクション（Actions）] 領域で、[リセット（Reset）] をクリックし、[はい（Yes）] をクリックして確定します。

（注） アダプタをリセットすると、ホストもリセットされ、再フォーマットが必要になります。

第 12 章

ストレージ アダプタの管理

この章の内容は、次のとおりです。

Managing Storage Adapters

自己暗号化ドライブ（フル ディスク暗号化）

Cisco IMC は、自己暗号化ドライブ（SED）をサポートしています。ドライブ内の特別なハードウェアがリアルタイムで入力データを暗号化し、出力データを復号します。この機能は、フルディスク暗号化（FDE）とも呼ばれます。

ドライブ上のデータは、ドライブに入力される際に暗号化され、出力される際に復号されます。ただし、ドライブをロックしている場合は、データを取得するためにセキュリティ キーは必要ありません。

ドライブがロックされると、暗号化キーが内部で作成され保存されます。このドライブに保存されているすべてのデータは、そのキーを使用して暗号化され、暗号化された形式で保存されます。データをこのように保存すると、データを非暗号化してドライブから取得するためにセキュリティ キーが必要になります。ドライブのロックを解除すると、その暗号化キーが削除され、保存されたデータは使用できなくなります。これは、Secure Erase と呼ばれます。FDE は、キー ID とセキュリティ キーで構成されます。

FDE 機能は次の操作をサポートしています。

- コントローラでのセキュリティの有効化および無効化
- セキュアな仮想ドライブの作成
- 非セキュアなドライブ グループの保護

- 外部の設定ドライブのロック解除
- 物理ドライブ（JBOD）でのセキュリティの有効化
- セキュアな SED ドライブのクリア
- セキュアな外部設定のクリア

デュアル SIOC 環境でコントローラ セキュリティを設定する場合に考慮すべきシナリオ

（注） デュアル SIOC 接続は一部のサーバでのみ使用できます。

コントローラ セキュリティは、個別に有効化、無効化、変更することができます。ただし、ローカルおよびリモート キー管理はサーバ上のすべてのコントローラに適用されます。したがって、キー管理モードの切り替えに関連するセキュリティ アクションは、慎重に実行する必要があります。両方のコントローラが保護されているシナリオにおいて、一方のコントローラを別のモードに切り替える場合は、もう一方のコントローラに対しても同じ操作を実行する必要があります。

次の 2 つのシナリオについて考えてください。

- シナリオ1：キー管理がリモートに設定されており、両方のコントローラが保護され、リモート キー管理を使用している。ローカル キー管理に切り替える場合は、各コントローラのキー管理を切り替えて、リモート キー管理を無効にします。
- シナリオ 2：キー管理がローカルに設定されており、両方のコントローラが保護され、ローカル キー管理を使用している。リモート キー管理に切り替える場合は、リモート キー管理を有効にして、各コントローラのキー管理を切り替えます。

どちらかのコントローラのセキュリティ方式を変更しないままにすると、セキュア キー管理が「サポートされない設定（unsupported configuration）」状態になります。

コントローラ セキュリティの有効化

このオプションを使用できるのは一部の C シリーズ サーバだけです。

はじめる前に

このタスクを実行するには、admin 権限で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 [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで、適切な LSI MegaRAID または HBA コントローラをクリックします。

ステップ 3 [コントローラ情報（Controller Info）] 領域で、[ドライブ セキュリティの有効化（Enable Drive Security）] をクリックします。

ステップ 4 [ドライブ セキュリティの有効化（Enable Drive Security）] 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（Name）]	説明
[コントローラ セキュリティ（Controller Security）] フィールド	コントローラが無効であることを示します。
[キー管理（Key Management）] フィールド	キーがリモート管理されるかローカル管理されるかを示します。次のいずれかになります。 • [リモート キー管理（Remote Key Management）] オプション ボタン：コントローラのセキュリティ キーが設定されているか、リモート KMIP サーバを使用して管理されています。 （注） このオプションを選択した場合、既存のセキュリティキーを指定する必要はありませんが、ローカル管理用のキー ID とセキュリティ キーを指定する必要があります。 • [ローカル キー管理（Local Key Management）] オプション ボタン：コントローラセキュリティがローカルに設定されています。
[セキュリティ キー ID（Security Key Identifier）] フィールド	現在のキー ID。
[セキュリティ キー（Security Key）] フィールド	コントローラ セキュリティを有効にするために使用されるセキュリティ キー。現在のセキュリティ キーを変更するには、ここに新しいキーを入力します。 （注） セキュリティ キーを変更すると、[セキュア キー検証（Secure Key Verification）] ポップアップ ウィンドウが表示され、確認のために現在のセキュリティ キーを入力する必要があります。

[名前（Name）]	説明
[セキュリティ キーの確認（Confirm Security Key）] フィールド	セキュリティ キーを再入力します。
[候補（Suggest）] ボタン	割り当てることができるセキュリティ キーまたはキー ID を提案します。

ステップ 5 [保存（Save）] をクリックします。
これにより、コントローラ セキュリティが有効になります。

コントローラ セキュリティの変更

このオプションを使用できるのは一部の C シリーズ サーバだけです。

はじめる前に

- このタスクを実行するには、admin 権限でログインする必要があります。
- コントローラ セキュリティを変更するには、最初にそれを有効化しておく必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで、適切な LSI MegaRAID または HBA コントローラをクリックします。

ステップ 3 [コントローラ情報（Controller Info）] 領域で、[ドライブ セキュリティの変更（Modify Drive Security）] をクリックします。

ステップ 4 [ドライブ セキュリティの変更（Modify Drive Security）] 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（Name）]	説明
[コントローラ セキュリティ（Controller Security）] フィールド	コントローラ セキュリティが有効かどうかを示します。次のいずれかになります。 • [はい（True）]：コントローラ セキュリティが有効です。 • [いいえ（False）]：コントローラ セキュリティが無効です。

[名前（Name）]	説明
[キー管理（Key Management）] フィールド	キーがリモート管理されるかローカル管理されるかを示します。次のいずれかになります。 • [リモート キー管理（Remote Key Management）] オプション ボタン：コントローラのセキュリティ キーが設定されているか、リモート KMIP サーバを使用して管理されています。 （注） このオプションを選択した場合、既存のセキュリティ キーを指定する必要はありませんが、ローカル管理用のキー ID とセキュリティ キーを指定する必要があります。 • [ローカル キー管理（Local Key Management）] オプション ボタン：コントローラ セキュリティがローカルに設定されています。
[セキュリティ キー ID（Security Key Identifier）] フィールド	現在のキー ID。
[セキュリティ キー（Security Key）] フィールド	コントローラ セキュリティを有効にするために使用されるセキュリティ キー。現在のセキュリティ キーを変更するには、ここに新しいキーを入力します。 （注） セキュリティ キーを変更すると、[セキュア キー検証（Secure Key Verification）] ポップアップ ウィンドウが表示され、確認のために現在のセキュリティ キーを入力する必要があります。
[セキュリティ キーの確認（Confirm Security Key）] フィールド	セキュリティ キーを再入力します。
[候補（Suggest）] ボタン	割り当てることができるセキュリティ キーまたはキー ID を提案します。
[保存（Save）] ボタン	データを保存します。
[キャンセル（Cancel）] ボタン	操作をキャンセルします。

ステップ 5 [保存（Save）] をクリックします。
これにより、コントローラ セキュリティの設定が変更されます。

コントローラ セキュリティの無効化

このオプションを使用できるのは一部の C シリーズ サーバだけです。

はじめる前に

- このタスクを実行するには、admin 権限でログインする必要があります。
- コントローラ セキュリティを無効化するには、最初にそれを有効化しておく必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで、適切な LSI MegaRAID または HBA コントローラをクリックします。

ステップ 3 [コントローラ情報（Controller Info）] 領域で、[ドライブ セキュリティの無効化（Disable Drive Security）] をクリックします。

ステップ 4 確認のポップアップ ウィンドウで [OK] をクリックします。
これにより、コントローラ セキュリティが無効化されます。

ローカル/リモート キー管理間でのコントローラ セキュリティの切り替え

このタスクによって、コントローラ セキュリティをローカル管理からリモート管理に切り替えたり、リモート管理からローカル管理に切り替えることができます。

はじめる前に

このタスクを実行するには、admin 権限で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 [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで、適切な LSI MegaRAID または HBA コントローラをクリックします。

ステップ 3 [コントローラ情報（Controller Info）] 領域で、コントローラ セキュリティをリモート管理からローカル管理に切り替えるには、[ローカル キー管理に切り替え（Switch to Local Key Management）] をクリックします。

（注） リモート キー管理からローカル キー管理に切り替える場合は、最初に KMIP セキュア キー管理を無効にしてください。

ステップ 4 （任意） 同様に、コントローラ セキュリティをローカル管理からリモート管理に切り替えるには、[リモート キー管理に切り替え（Switch to Remote Key Management）] をクリックします。

ステップ 5 [OK] をクリックして確認します。

未使用の物理ドライブからの仮想ドライブの作成

はじめる前に

このタスクを実行するには、admin 権限で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 [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで、適切な LSI MegaRAID または HBA コントローラをクリックします。

ステップ 3 [アクション（Actions）] 領域で、[未使用の物理ドライブからの仮想ドライブの作成（Create Virtual Drive from Unused Physical Drives）] をクリックします。
[未使用の物理ドライブからの仮想ドライブの作成（Create Virtual Drive from Unused Physical Drives）] ダイアログボックスが表示されます。

ステップ 4 [未使用の物理ドライブからの仮想ドライブの作成（Create Virtual Drive from Unused Physical Drives）] ダイアログボックスで、新しい仮想ドライブの RAID レベルを選択します。
次のいずれかになります。

- [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]：パリティ付きのスパンされたストライピング。
- [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。

ステップ 5 [ドライブ グループの作成（Create Drive Groups）] 領域で、グループに含める 1 つ以上の物理ドライブを選択します。
[ドライブ グループ（Drive Groups）] テーブルにドライブを追加するには、[>>] ボタンを使用します。ドライブ グループから物理ドライブを削除するには、[<<] ボタンを使用します。

（注） ドライブ グループで最も小さな物理ドライブのサイズによって、すべての物理ドライブに使用される最大サイズが定義されます。すべての物理ドライブの領域の最大使用を保証するには、ドライブ グループ内のすべてのドライブのサイズをほぼ同じにすることを推奨します。

（注） Cisco IMC は、RAID コントローラのみを管理し、サーバに接続された HBA は管理しません。

ステップ 6 [仮想ドライブ プロパティ（Virtual Drive Properties）] 領域で、次のプロパティを更新します。

[名前（Name）]	**説明**
[仮想ドライブ名（Virtual Drive Name）] フィールド	作成する新しい仮想ドライブの名前。
[読み取りポリシー（Read Policy）] ドロップダウン リスト	先行読み出しキャッシュ モード。
[キャッシュ ポリシー（Cache Policy）] ドロップダウン リスト	バッファリング読み取りに使用されるキャッシュ ポリシー。
[ストライプ サイズ（Strip Size）] ドロップダウン リスト	各ストライプのサイズ（KB 単位）。
[書き込みポリシー（Write Policy）] ドロップダウン リスト	次のいずれかになります。 • [書き込みスルー（Write Through）]：データがキャッシュによって、物理ドライブに書き込まれます。以降の該当データのキャッシュからの読み取りが充足されるため、パフォーマンスが改善されます。 • [書き込みバック（Write Back）]：データはキャッシュに保存され、キャッシュ内の領域が必要になったときにのみ、物理ドライブに書き込まれます。このポリシーを必要とする仮想ドライブは、電源障害の発生時にBBUでキャッシュの安全性を確保できない場合、[書き込みスルー（Write Through）] キャッシングにフォールバックします。 • [書き込みバック不良 BBU（Write Back Bad BBU）]：このポリシーでは、バッテリ バックアップ ユニットに欠陥があったり、放電していたりする場合でも、書き込みキャッシングは [書き込みバック（Write Back）] のままです。

[名前（Name）]	説明
[ディスク キャッシュ ポリシー（Disk Cache Policy）] ドロップダウン リスト	次のいずれかになります。 • [未変更（Unchanged）]：ディスク キャッシュ ポリシーは変更されません。 • [有効（Enabled）]：ディスクで IO キャッシングを許可します。 • [無効（Disabled）]：ディスク キャッシングを許可しません。
[アクセス ポリシー（Access Policy）] ドロップダウン リスト	次のいずれかになります。 • [読み取り/書き込み（Read Write）]：ホストが VD で読み取り/書き込みを実行できます。 • [読み取り専用（Read Only）]：ホストは VD から読み取りのみ行うことができます。 • [ブロック済み（Blocked）]：ホストは VD の読み取りおよび書き込みができません。
[サイズ（Size）] フィールド	作成する仮想ドライブのサイズ。値を入力し、次のいずれかの単位を選択します。 • [MB] • GB • [TB]

ステップ 7 [XML API 要求の生成（Generate XML API Request）] ボタンをクリックして、API 要求を生成します。

ステップ 8 [閉じる（Close）] をクリックします。

ステップ 9 [仮想ドライブの作成（Create Virtual Drive）] をクリックします。

既存のドライブ グループからの仮想ドライブの作成

はじめる前に

このタスクを実行するには、admin 権限で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 [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで、適切な LSI MegaRAID または HBA コントローラをクリックします。

ステップ 3 [アクション（Actions）] 領域で、[既存の仮想ドライブ グループからの仮想ドライブの作成（Create Virtual Drive from an Existing Virtual Drive Group）] をクリックします。
[既存の仮想ドライブ グループからの仮想ドライブの作成（Create Virtual Drive from an Existing Virtual Drive Group）] ダイアログボックスが表示されます。

ステップ 4 [既存の仮想ドライブ グループからの仮想ドライブの作成（Create Virtual Drive from an Existing Virtual Drive Group）] ダイアログボックスで、新しい仮想ドライブの作成に使用するドライブ グループの仮想ドライブを選択します。

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

[名前（Name）]	**説明**
[仮想ドライブ名（Virtual Drive Name）] フィールド	作成する新しい仮想ドライブの名前。
[読み取りポリシー（Read Policy）] ドロップダウン リスト	先行読み出しキャッシュ モード。
[キャッシュ ポリシー（Cache Policy）] ドロップダウン リスト	バッファリング読み取りに使用されるキャッシュ ポリシー。
[ストライプ サイズ（Strip Size）] ドロップダウン リスト	各ストライプのサイズ（KB 単位）。

[名前（Name）]	説明
[書き込みポリシー（Write Policy）] ドロップダウン リスト	次のいずれかになります。 • [書き込みスルー（Write Through）]：データがキャッシュによって、物理ドライブに書き込まれます。以降の該当データのキャッシュからの読み取りが充足されるため、パフォーマンスが改善されます。 • [書き込みバック（Write Back）]：データはキャッシュに保存され、キャッシュ内の領域が必要になったときにのみ、物理ドライブに書き込まれます。このポリシーを必要とする仮想ドライブは、電源障害の発生時にBBUでキャッシュの安全性を確保できない場合、[書き込みスルー（Write Through）] キャッシングにフォールバックします。 • [書き込みバック不良 BBU（Write Back Bad BBU）]：このポリシーでは、バッテリ バックアップ ユニットに欠陥があったり、放電していたりする場合でも、書き込みキャッシングは [書き込みバック（Write Back）] のままです。
[ディスク キャッシュ ポリシー（Disk Cache Policy）] ドロップダウン リスト	次のいずれかになります。 • [未変更（Unchanged）]：ディスク キャッシュ ポリシーは変更されません。 • [有効（Enabled）]：ディスクで IO キャッシングを許可します。 • [無効（Disabled）]：ディスク キャッシングを許可しません。
[アクセス ポリシー（Access Policy）] ドロップダウン リスト	次のいずれかになります。 • [読み取り/書き込み（Read Write）]：ホストが VD で読み取り/書き込みを実行できます。 • [読み取り専用（Read Only）]：ホストは VD から読み取りのみ行うことができます。 • [ブロック済み（Blocked）]：ホストは VD の読み取りおよび書き込みができません。

[名前（Name）]	説明
[サイズ（Size）] フィールド	作成する仮想ドライブのサイズ。値を入力し、次のいずれかの単位を選択します。 • [MB] • GB • [TB]

ステップ 6 [XML API 要求の生成（Generate XML API Request）] ボタンをクリックして、API 要求を生成します。

ステップ 7 [閉じる（Close）] をクリックします。

ステップ 8 [仮想ドライブの作成（Create Virtual Drive）] をクリックします。

仮想ドライブのトランスポート可能状態の設定

仮想ドライブを MegaRAID コントローラ間で移動するには、[トランスポート可能状態の設定（Set Transport Ready）] 機能を使用します。この機能を使用すると、仮想ドライブの保留中 IO アクティビティがすべて完了されてから仮想ドライブがオペレーティング システムから隠され、キャッシュがフラッシュされ、すべてのバックグラウンド操作が一時停止された後、現在の進行状況がディスク データ フォーマットに保存されます。これにより、ドライブを移動することが可能になります。仮想ドライブを移動すると、その仮想ドライブと同じドライブ グループに属する他のすべてのドライブが移動されたドライブと同じ変更を継承します。

グループに設定された最後の物理ドイブが現在のコントローラから除去されると、そのドライブ グループは外部ドライブ グループとなり、外部構成ルールのすべてが適用されます。ただし、トランスポート準備機能によって外部構成の動作が変更されることはありません。

仮想ドライブをトランスポート可能状態から解除することもできます。これにより、仮想ドライブがオペレーティング システムで使用可能になります。

トランスポート可能状態の仮想ドライブには、次の制限が適用されます。

- 現在、最大で 16 個のトランスポート可能状態のドライブ グループがサポートされています。
- この機能は、ハイ アベイラビリティ構成ではサポートされません。
- 次の場合は、仮想ドライブをトランスポート可能状態に設定することはできません。
  - ドライブ グループの仮想ドライブが再構成中の場合
  - ドライブ グループの仮想ドライブに固定キャッシュが含まれている場合
  - ドライブ グループの仮想ドライブがキャッシュ可能としてマークされているか、CacheCade 仮想ドライブに関連付けられている場合

- 仮想ドライブが CacheCade 仮想ドライブの場合
- 仮想ドライブがオフラインの場合
- 仮想ドライブがブート可能な仮想ドライブの場合

トランスポート可能としての仮想ドライブの設定

はじめる前に

- このタスクを実行するには、admin 権限でログインする必要があります。
- 仮想ドライブをトランスポート可能にするには、仮想ドライブが最適な状態になっていなければなりません。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで、該当する LSI MegaRAID または HBA コントローラをクリックします。

ステップ 3 [作業（Work）] ペインで [仮想ドライブ情報（Virtual Drive Info）] タブをクリックします。

ステップ 4 [仮想ドライブ（Virtual Drives）] 領域で、トランスポート可能として設定するドライブを選択します。

ステップ 5 [アクション（Actions）] 領域で、[トランスポート可能状態の設定（Set Transport Ready）] をクリックします。
[トランスポート可能状態の設定（Set Transport Ready）] ダイアログボックスが表示されます。

ステップ 6 このダイアログボックスで次のプロパティを更新します。

[名前（Name）]	**説明**
[初期化タイプ（Initialize Type）] ドロップダウン リスト	選択した仮想ドライブをトランスポート可能として設定するために使用する初期化タイプを選択できます。次のいずれかになります。 • [すべて除外する（Exclude All）]：専用ホットスペア ドライブをすべて除外します。 • [すべて含める（Include All）]：排他的に使用可能な専用ホットスペア ドライブまたは共有される専用ホットスペア ドライブをすべて含めます。 • [専用ホット スペア ドライブを含める（Include Dedicated Hot Spare Drive）]：排他的に使用可能な専用ホットスペア ドライブを含めます。

[名前（Name）]	説明
[トランスポート可能状態の設定（Set Transport Ready）] ボタン	選択した仮想ドライブをトランスポート可能として設定します。
[キャンセル（Cancel）] ボタン	操作をキャンセルします。

（注） 仮想ドライブをトランスポート可能として設定すると、その仮想ドライブに関連付けられているすべての物理ドライブが [削除準備完了（Ready to Remove）] として表示されます。

仮想ドライブのトランスポート可能状態の解除

はじめる前に

- このタスクを実行するには、admin 権限でログインする必要があります。
- 仮想ドライブがトランスポート可能状態になっている必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで、該当する LSI MegaRAID または HBA コントローラをクリックします。

ステップ 3 [作業（Work）] ペインで [仮想ドライブ情報（Virtual Drive Info）] タブをクリックします。

ステップ 4 [仮想ドライブ（Virtual Drives）] 領域でトランスポート可能として設定されているドライブを選択します。

ステップ 5 [アクション（Actions）] 領域で、[トランスポート可能状態のクリア（Clear Transport Ready）] をクリックします。
これにより、選択したトランスポート可能な仮想ドライブが元の最適な状態に戻されます。

外部設定のインポート

別のコントローラで以前に設定されている 1 つ以上の物理ドライブがサーバにインストールされると、それらは外部設定として識別されます。コントローラにこれらの外部設定をインポートできます。

重要 次の 2 つのシナリオでは、外部設定をインポートできません。

1. セキュアな仮想ドライブがサーバ 1（設定のインポート元）でリモート キーを使用して作成された場合、およびサーバ 2（設定のインポート先）でローカル キーを使用して作成された場合。
2. サーバ 1 の KMIP サーバ クラスタに属していない別の KMIP サーバが、サーバ 2 に設定されている場合。

これらのシナリオに外部設定をインポートするには、サーバ 2 のコントローラ セキュリティをローカル キー管理からリモート キー管理に変更し、サーバ 1 の KMIP が設定されている同じクラスタの同じ KMIP サーバを使用します。

はじめる前に

このタスクを実行するには、admin 権限で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 [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [RAID コントローラ（RAID Controller）] 領域に、デフォルトで [コントローラ情報（Controller Info）] タブが表示されます。

ステップ 3 [アクション（Actions）] 領域で、[外部設定のインポート（Import Foreign Config）] をクリックします。

（注） KMIP が有効でない場合は、[セキュア キー検証（Secure Key Verification）] ダイアログボックスが表示され、外部設定のインポート プロセスを開始するためにセキュリティ キーの入力を求められます。

KMIP が有効な場合は、[セキュア キー検証（Secure Key Verification）] ダイアログボックスに次のようなメッセージが表示されます。「ドライブのセキュリティがリモート キー管理により有効になっている場合、セキュリティ キーの指定は任意です（If drive security has been enabled via remote key management, specifying Security key is optional.）。外部設定のインポートを開始するには、*[*検証（*verify*）*]* をクリックしてください（*Click on verify to start foreign configuration import.*）」

これにより、セキュリティ キーを入力せずに、[検証（verify）] をクリックしてインポートを開始できます。

ステップ 4 [OK] をクリックして確認します。

外部設定のクリア

重要　このタスクでは、コントローラのすべての外部設定をクリアします。また、外部設定をホスティングしているすべての物理ドライブからすべての設定情報が削除されます。このアクションは元に戻せません。

はじめる前に

このタスクを実行するには、admin 権限で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 [ストレージ（Storage）] メニューをクリックします。

ステップ 2　[ストレージ（Storage）] メニューで、該当する LSI MegaRAID または HBA コントローラをクリックします。
[RAID コントローラ（RAID Controller）] 領域に、デフォルトで [コントローラ情報（Controller Info）] タブが表示されます。

ステップ 3　[アクション（Actions）] 領域で、[外部設定のクリア（Clear Foreign Config）] をクリックします。

ステップ 4　[OK] をクリックして確認します。

ブート ドライブのクリア

重要　このタスクでは、コントローラのブート ドライブ設定がクリアされます。このアクションは元に戻せません。

はじめる前に

このタスクを実行するには、admin 権限で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 [ストレージ（Storage）] メニューをクリックします。

ステップ 2　[ストレージ（Storage）] メニューで、該当する LSI MegaRAID または HBA コントローラをクリックします。

[RAID コントローラ（RAID Controller）] 領域に、デフォルトで [コントローラ情報（Controller Info）] タブが表示されます。

ステップ 3 [アクション（Actions）] 領域で、[ブート ドライブのクリア（Clear Boot Drive）] をクリックします。

ステップ 4 [OK] をクリックして確認します。

JBOD モードのイネーブル化

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで、該当する LSI MegaRAID または HBA コントローラをクリックします。

ステップ 3 [RAID コントローラ（RAID Controller）] 領域で、[物理ドライブ情報（Physical Drive Info）] タブをクリックします。

ステップ 4 [物理ドライブ（Physical Drives）] 領域で、未設定の適切なドライブを選択します。

ステップ 5 [アクション（Actions）] 領域で [JBOD の有効化（Enable JBOD）] 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。

JBOD のディセーブル化

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

はじめる前に

JBOD オプションは、選択したコントローラに対してイネーブルに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 [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで、該当する LSI MegaRAID または HBA コントローラをクリックします。

ステップ 3 [RAID コントローラ（RAID Controller）] 領域で、[物理ドライブ情報（Physical Drive Info）] タブをクリックします。

ステップ 4 [物理ドライブ（Physical Drives）] 領域で、JBOD ドライブを選択します。

ステップ 5 [アクション（Actions）] 領域で [JBOD の無効化（Disable JBOD）] 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。

コントローラのストレージ ファームウェア ログの取得

このタスクでは、コントローラのストレージ ファームウェア ログを取得して `/var/log` に配置します。これにより、テクニカル サポート データが要求された場合にこのログ データを確実に使用できるようになります。

はじめる前に

このタスクを実行するには、admin 権限で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 [ストレージ（Storage）] メニューをクリックします。

ステップ 2 作業領域に、デフォルトで [コントローラ情報（Controller Info）] タブが表示されます。

ステップ 3 [アクション（Actions）] 領域で、[ストレージ ファームウェア ログの取得（Get Storage Firmware Log）] をクリックします。

ステップ 4 [OK] をクリックして確認します。

重要 コントローラのストレージ ファームウェア ログの取得には、2 ～ 4 分かかることがあります。このプロセスが完了するまで、テクニカル サポート データのエクスポートを開始しないでください。

コントローラの設定のクリア

はじめる前に

このタスクを実行するには、admin 権限で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 [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで、適切な LSI MegaRAID または HBA コントローラをクリックします。

ステップ 3 [コントローラ情報（Controller Info）] 領域で、[すべての設定をクリア（Clear All Configuration）] をクリックします。

ステップ 4 [OK] をクリックして確認します。
これにより、既存のコントローラ設定がクリアされます。

工場出荷時の初期状態にストレージ コントローラを復元

はじめる前に

このタスクを実行するには、admin 権限で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 [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで、適切な LSI MegaRAID または HBA コントローラをクリックします。

ステップ 3 [コントローラ情報（Controller Info）] 領域で、[工場出荷時の初期状態に設定（Set Factory Defaults）] をクリックします。

ステップ 4 [OK] をクリックして確認します。
これにより、コントローラの設定が工場出荷時の初期状態に復元されます。

削除するドライブの準備

（注） [未設定良好（Unconfigured Good）] ステータスを表示する物理ドライブのみでこのタスクを実行できます。

はじめる前に

このタスクを実行するには、admin 権限で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 [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで、該当する LSI MegaRAID または HBA コントローラをクリックします。

ステップ 3 [RAID コントローラ（RAID Controller）] 領域で、[物理ドライブ情報（Physical Drive Info）] タブをクリックします。

ステップ 4 [物理ドライブ（Physical Drives）] 領域で、削除するドライブを選択します。

ステップ 5 [アクション（Actions）] 領域で、[削除の準備（Prepare for Removal）] をクリックします。

ステップ 6 [OK] をクリックして確認します。

削除するドライブの準備の取り消し

はじめる前に

このタスクを実行するには、admin 権限で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 [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで、該当する LSI MegaRAID または HBA コントローラをクリックします。

ステップ 3 [RAID コントローラ（RAID Controller）] 領域で、[物理ドライブ情報（Physical Drive Info）] タブをクリックします。

ステップ 4 [物理ドライブ（Physical Drives）] 領域で、[削除準備完了（Ready to Remove）] 状態のドライブを選択します。

ステップ 5 [アクション（Actions）] 領域で、[削除の準備の取り消し（Undo Prepare for Removal）] をクリックします。

ステップ 6 [OK] をクリックして確認します。

専用ホット スペアの作成

はじめる前に

このタスクを実行するには、admin 権限で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 [ストレージ（Storage）] タブをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで、該当する LSI MegaRAID または HBA コントローラをクリックします。

ステップ 3 [RAID コントローラ（RAID Controller）] 領域で、[物理ドライブ情報（Physical Drive Info）] タブをクリックします。

ステップ 4 [物理ドライブ（Physical Drives）] 領域で、専用ホット スペアを作成する未設定の適切なドライブを選択します。

ステップ 5 [アクション（Actions）] 領域で、[専用ホット スペアの作成（Make Dedicated Hot Spare）] をクリックします。
[専用ホット スペアの作成（Make Dedicated Hot Spare）] ダイアログボックスが表示されます。

ステップ 6 [仮想ドライブの詳細（Virtual Drive Details）] 領域で、次のプロパティを更新します。

[名前（Name）]	説明
[仮想ドライブ番号（Virtual Drive Number）] ドロップダウン リスト	ホット スペアとして物理ドライブを専用する仮想ドライブを選択します。
[仮想ドライブ名（Virtual Drive Name）] フィールド	選択された仮想ドライブの名前。
[専用ホット スペアの作成（Make Dedicated Hot Spare）] ボタン	専用のホット スペアを作成します。
[キャンセル（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。

ステップ 7 [専用ホット スペアの作成（Make Dedicated Hot Spare）] をクリックして確定します。

グローバル ホット スペアの作成

はじめる前に

このタスクを実行するには、admin 権限で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 [ストレージ（Storage）] タブをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで、該当する LSI MegaRAID または HBA コントローラをクリックします。

ステップ 3 [RAID コントローラ（RAID Controller）] 領域で、[物理ドライブ情報（Physical Drive Info）] タブをクリックします。

ステップ 4 [物理ドライブ（Physical Drives）] 領域で、グローバル ホット スペアを作成する未設定の適切なドライブを選択します。

ステップ 5 [アクション（Actions）] 領域で、[グローバル ホット スペアの作成（Make Global Hot Spare）] をクリックします。

ホット スペア プールからのドライブの削除

はじめる前に

このタスクを実行するには、admin 権限で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 [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [ストレージ（Storage）] タブで、適切な LSI MegaRAID コントローラをクリックします。

ステップ 3 [作業（Work）] ペインで [物理ドライブ情報（Physical Drive Info）] タブをクリックします。

ステップ 4 [物理ドライブ（Physical Drives）] 領域で、ホット スペア プールから削除するグローバル ホット スペアまたは専用ホット スペアを選択します。

ステップ 5 [アクション（Actions）] 領域で、[ホット スペア プールからの削除（Remove From Hot Spare Pools）] をクリックします。

物理ドライブのステータスの切り替え

はじめる前に

- このタスクを実行するには、admin 権限でログインする必要があります。
- コントローラは、JBOD モードをサポートする必要があり、JBOD モードはイネーブルに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 [ストレージ（Storage）] タブをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで、該当する LSI MegaRAID または HBA コントローラをクリックします。

ステップ 3 [RAID コントローラ（RAID Controller）] 領域で、[物理ドライブ情報（Physical Drive Info）] タブをクリックします。

ステップ 4 [物理ドライブ（Physical Drives）] 領域で、未設定良好として設定するドライブを選択します。

ステップ 5 [アクション（Actions）] 領域で、[状態を未設定の良好に設定する（Set State as Unconfigured Good）] をクリックします。

ステップ 6 [OK] をクリックして、JBOD モードがディセーブルになっていることを確認します。
[状態を JBOD として設定する（Set State as JBOD）] オプションがイネーブルになります。

ステップ 7 物理ドライブの JBOD モードをイネーブルにするには、[状態を JBOD として設定する（Set State as JBOD）] をクリックします。

ステップ 8 [OK] をクリックして確認します。
[状態を未設定の良好に設定する（Set State as Unconfigured Good）] オプションがイネーブルになります。

コントローラのブート ドライブとしての物理ドライブの設定

はじめる前に

- このタスクを実行するには、admin 権限でログインする必要があります。
- コントローラは、JBOD モードをサポートする必要があり、JBOD モードはイネーブルに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 [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで、該当する LSI MegaRAID または HBA コントローラをクリックします。

ステップ 3 [RAID コントローラ（RAID Controller）] 領域で、[物理ドライブ情報（Physical Drive Info）] タブをクリックします。

ステップ 4 [物理ドライブ（Physical Drives）] 領域で、コントローラのブート ドライブとして設定するドライブを選択します。

ステップ 5 [アクション（Actions）] 領域で、[ブート ドライブとしての設定（Set as Boot Drive）] をクリックします。

ステップ 6 [OK] をクリックして確認します。

仮想ドライブの初期化

ドライブを初期化すると、仮想ドライブ上のすべてのデータが失われます。初期化を実行する前に、保存する仮想ドライブのデータをバックアップします。

はじめる前に

このタスクを実行するには、admin 権限で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 [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで、該当する LSI MegaRAID または HBA コントローラをクリックします。

ステップ 3 [RAID コントローラ（RAID Controller）] 領域で、[仮想ドライブ情報（Virtual Drive Info）] タブをクリックします。

ステップ 4 [仮想ドライブ（Virtual Drives）] 領域で、初期化するドライブを選択します。

ステップ 5 [アクション（Actions）] 領域で、[初期化（Initialize）] をクリックします。
[仮想ドライブの初期化（Initialize Virtual Drive）] ダイアログボックスが表示されます。

ステップ 6 仮想ドライブに使用する初期化のタイプを選択します。
次のいずれかになります。

- [高速初期化（Fast Initialize）]：このオプションは、仮想ドライブへのデータの書き込みをすぐに開始できます。
- [完全な初期化（Full Initialize）]：新しい設定で完全な初期化が実行されます。初期化が完了するまで、新しい仮想ドライブにデータを書き込むことができません。

ステップ 7 [VD の初期化（Initialize VD）] をクリックしてドライブを初期化するか、[キャンセル（Cancel）] をクリックして、変更を行わずにダイアログボックスを閉じます。

ステップ 8 ドライブで実行しているタスクのステータスを表示するには、[操作（Operations）] 領域で [更新（Refresh）] をクリックします。
次の詳細情報が表示されます。

[名前（Name）]	説明
操作	ドライブで進行中の操作の名前。
[進行状況 %（Progress in %）]	操作の進行状況（完了した割合）。
[経過時間（秒）（Elapsed Time in secs）]	操作開始から経過した時間（秒数）。

ブート ドライブとしての設定

はじめる前に

このタスクを実行するには、admin 権限で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 [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで、該当する LSI MegaRAID または HBA コントローラをクリックします。

ステップ 3 [RAID コントローラ（RAID Controller）] 領域で、[仮想ドライブ情報（Virtual Drive Info）] タブをクリックします。

ステップ 4 [仮想ドライブ（Virtual Drives）] 領域で、コントローラが起動する必要のあるドライブを選択します。

ステップ 5 [アクション（Actions）] 領域で、[ブート ドライブとしての設定（Set as Boot Drive）] をクリックします。

ステップ 6 [OK] をクリックして確認します。

仮想ドライブの編集

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで、該当する LSI MegaRAID または HBA コントローラをクリックします。

ステップ 3 [RAID コントローラ（RAID Controller）] 領域で、[仮想ドライブ情報（Virtual Drive Info）] タブをクリックします。

ステップ 4 [仮想ドライブ（Virtual Drives）] 領域で、[仮想ドライブの編集（Edit Virtual Drive）] をクリックします。

ステップ 5 この説明を確認してから、[OK] をクリックします。
[仮想ドライブの編集（Edit Virtual Drive）] ダイアログボックスが表示され、データをバックアップするよう指示されます。

ステップ 6 [移行する RAID レベルを選択（Select RAID Level to migrate）] ドロップダウン リストから、RAID レベルを選択します。
RAID のマイグレーション基準については次の表を参照してください。

[名前（Name）]	説明
[移行する RAID レベルを選択（Select RAID Level to migrate）] ドロップダウン リスト	移行する RAID レベルを選択します。移行は次の RAID レベルで許可されています。 • [RAID 0] から [RAID 1] へ • [RAID 0] から [RAID 5] へ • [RAID 0] から [RAID 6] へ • [RAID 1] から [RAID 0] へ • [RAID 1] から [RAID 5] へ • [RAID 1] から [RAID 6] へ • [RAID 5] から [RAID 0] へ • [RAID 6] から [RAID 0] へ • [RAID 6] から [RAID 5] へ ある raid レベルから別のレベルに移行する場合、新しい RAID レベルのデータ アームは、既存のもの以上である必要があります。 RAID 6 の場合、RAID 6 には二重分散パリティがあるため、データ アームはドライブ数から 2 を引いた数になります。たとえば、8 台のドライブで RAID 6 を作成する場合、データ アームの数は 8 – 2 = 6 となります。この場合、RAID 6 から RAID 0 に移行する場合は、RAID 0 には最低 6 台のドライブが必要です。それより少ないドライブ数を選択すると、[編集（Edit）] または [保存（Save）] ボタンが無効になります。 追加する場合は、ドライブを削除しないままで RAID 0 に移行できます。 （注） RAID レベルの移行は、次の場合にはサポートされません。 • RAID グループに複数の仮想ドライブがある場合。 • SSD/HDD RAID グループの組み合わせがある場合。

ステップ 7 [仮想ドライブ プロパティ（Virtual Drive Properties）] 領域の [書き込みポリシー（Write Policy）] ドロップダウン リストから、次のいずれかを選択します。

- [書き込みスルー（Write Through）]：データがキャッシュによって、物理ドライブに書き込まれます。以降の該当データのキャッシュからの読み取りが充足されるため、パフォーマンスが改善されます。
- [書き込みバック（Write Back）]：データはキャッシュに保存され、キャッシュ内の領域が必要になったときにのみ、物理ドライブに書き込まれます。このポリシーを必要とする仮想ドライブは、電源障害の発生時に BBU でキャッシュの安全性を確保できない場合、[書き込みスルー（Write Through）] キャッシングにフォールバックします。
- [書き込みバック不良 BBU（Write Back Bad BBU）]：このポリシーでは、バッテリ バックアップ ユニットに欠陥があったり、放電していたりする場合でも、書き込みキャッシングは [書き込みバック（Write Back）] のままです。

ステップ 8 [変更の保存（Save Changes）] をクリックします。

仮想ドライブの削除

重要 このタスクでは、ブートされたオペレーティング システムを実行するドライブを含む仮想ドライブを削除します。そのため、仮想ドライブを削除する前に、保持するデータをバックアップします。

はじめる前に

このタスクを実行するには、admin 権限で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 [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで、該当する LSI MegaRAID または HBA コントローラをクリックします。

ステップ 3 [RAID コントローラ（RAID Controller）] 領域で、[仮想ドライブ情報（Virtual Drive Info）] タブをクリックします。

ステップ 4 [仮想ドライブ（Virtual Drives）] 領域で、削除する仮想ドライブを選択します。

ステップ 5 [アクション（Actions）] 領域で、[仮想ドライブの削除（Delete Virtual Drive）] をクリックします。

ステップ 6 [OK] をクリックして確認します。

仮想ドライブの非表示

はじめる前に

このタスクを実行するには、admin 権限で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 [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで、該当する LSI MegaRAID または HBA コントローラをクリックします。

ステップ 3 [RAID コントローラ（RAID Controller）] 領域で、[仮想ドライブ情報（Virtual Drive Info）] タブをクリックします。

ステップ 4 [仮想ドライブ（Virtual Drives）] 領域で、非表示にする仮想ドライブを選択します。

ステップ 5 [アクション（Actions）] 領域で、[ドライブの非表示（Hide Drive）] をクリックします。

ステップ 6 [OK] をクリックして確認します。

バッテリ バックアップ ユニットの学習サイクルの開始

はじめる前に

このタスクを実行するには、admin 権限で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 [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで、該当する LSI MegaRAID または HBA コントローラをクリックします。

ステップ 3 [RAID コントローラ（RAID Controller）] 領域で、[バッテリ バックアップ ユニット（Battery Backup Unit）] タブをクリックします。

ステップ 4 [アクション（Actions）] ペインで [学習サイクルの開始（Start Learn Cycle）] をクリックします。ダイアログでタスクを確認するためのプロンプトが表示されます。

ステップ 5 [OK] をクリックします。

ストレージ コントローラのログの表示

はじめる前に

このタスクを実行するには、admin 権限で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 [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで、該当する LSI MegaRAID または HBA コントローラをクリックします。

ステップ 3 [RAID コントローラ（RAID Controller）] 領域で、[ストレージ ログ（Storage Log）] タブをクリックして次の情報を確認します。

[名前（Name）]	**説明**
[時刻（Time）] カラム	イベントが発生した日時。
[重大度（Severity）] カラム	イベントの重大度。次のいずれかになります。 • 緊急（Emergency） • アラート（Alert） • クリティカル（Critical） • エラー（Error） • 警告 • 通知（Notice） • 情報（Informational） • デバッグ（Debug）
[説明（Description）] カラム	イベントの説明。

MegaRAID コントローラの SSD スマート情報の表示

ソリッド ステート ドライブのスマート情報を表示できます。次の手順を実行します。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ストレージ（Storage）] タブをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで、適切な LSI MegaRAID コントローラをクリックします。

ステップ 3 [作業（Work）] ペインで [物理ドライブ情報（Physical Drive Info）] タブをクリックします。

ステップ 4 [スマート情報（Smart Information）] 領域で、次の情報を確認します。

[名前（Name）]	説明
[電源の再投入回数（Power Cycle Count）] フィールド	製造された時点からドライブの電源が再投入された回数。
[電源オンの時間数（Power on Hours）] フィールド	ドライブが「電源オン」モードにある時間の合計数。
[残りのライフのパーセンテージ（Percentage Life Left）] フィールド	ソリッドステートドライブ（SSD）に残っている書き込みサイクル数。たとえば、SSD がライフタイム中に 100 の書き込みサイクルに対応でき、15 の書き込みを完了している場合、ドライブの残りのライフのパーセンテージは 85% です。各パーセンテージの範囲が異なる色で表されます。たとえば、75% ～ 100% は緑、1 ～ 25% は赤で示されます。
[消耗状態（日数）（Wear Status in Days）] フィールド	SSD が書き込みサイクルを実行した日数。 SSD ベンダーによって、SSD での 1 日あたりの有限書き込み数が提示されます。その数に基づいて、SSD が動作し続ける総年数を計算できます。
[動作温度（Operating Temperature）] フィールド	選択した SSD が選択時点で動作しているドライブの現在の温度。
[使用された予約済み容量の割合（Percentage Reserved Capacity Consumed）] フィールド	SSD で使用された総容量（予約されている割合の内）。
[最終更新時間（Time of Last Refresh）] フィールド	ドライブが最後に更新された時間帯。

Managing the Flexible Flash Controller

Cisco Flexible Flash

C シリーズラックマウントサーバによっては、サーバソフトウェアツールおよびユーティリティのストレージとして、内蔵 Secure Digital（SD）メモリ カードをサポートしています。この SD カードは Cisco Flexible Flash ストレージ アダプタでホストされます。

Cisco IMC では、単一ハイパーバイザ（HV）パーティション設定として SD ストレージが使用可能です。以前のバージョンでは 4 つの仮想 USB ドライブがありました。3 つには Cisco UCS Server Configuration Utility、Cisco ドライバ、および Cisco Host Upgrade Utility が事前ロードされ、4 番目はユーザ インストールによるハイパーバイザでした。また、Cisco IMC の最新バージョンにアップグレードするか、旧バージョンにダウングレードした後、設定をリセットした場合にも、単一 HV パーティション設定が作成されます。

シスコ ソフトウェア ユーティリティおよびパッケージの詳細については、次の URL の『*Cisco UCS C-Series Servers Documentation Roadmap*』を参照してください。

http://www.cisco.com/go/unifiedcomputing/c-series-doc

Cisco Flexible Flash コントローラのカード管理機能

Cisco Flexible Flash コントローラでは、単一のカードに加えて 2 つの SD カードを RAID-1 ペアとして管理できます。カード管理機能の導入により、次の作業を実行できます。

（注）

- バージョン 1.4(5e) から 1.5(4) 以降のバージョンにアップグレードする場合は、まずバージョン 1.5(2) にアップグレードしてから、Cisco IMC の上位バージョンにアップグレードする必要があります。
- すべての Cisco IMC ファームウェアのアップグレード後に、最新の Flex Flash ファームウェアをロードするには、Cisco Flexible Flash コントローラをリセットします。

アクション	説明
Cisco Flex Flash のリセット（Reset Cisco Flex Flash）	コントローラをリセットできます。
パーティション デフォルトのリセット（Reset Partition Defaults）	選択したスロットの設定をデフォルト設定にリセットできます。
カード設定の同期（Synchronize Card Configuration）	ファームウェア バージョン 253 以降をサポートする SD カードの設定を保持できます。
運用プロファイルの設定（Configure Operational Profile）	選択した Cisco Flexible Flash コントローラの SD カードを設定できます。

RAID パーティションの列挙

非 RAID パーティションは常にプライマリ カードから列挙されます。列挙はプライマリ カードのステータスに依存しません。

次に、Cisco Flexible Flash コントローラに 2 枚のカードがあるときの RAID パーティションの列挙の動作を示します。

シナリオ	動作
シングル カード	RAID パーティションは、カードが正常に動作している場合、およびモードが [プライマリ（Primary）] または [セカンダリ アクティブ（Secondary-active）] の場合に列挙されます。
デュアル ペア カード	RAID パーティションは、カードの 1 つが正常に動作していれば列挙されます。 1 枚のカードだけが正常に動作している場合、すべての読み取り/書き込み操作は、この正常に動作しているカードで行われます。2 つの RAID パーティションを同期するには UCS SCU を使用する必要があります。
デュアル非ペア カード	サーバを再起動するときにこのシナリオが検出された場合、RAID パーティションはいずれも列挙されません。 サーバが稼働しているときにこのシナリオが検出された場合、ユーザが新しい SD カードを取り付けても、そのカードは Cisco Flexible Flash コントローラによって管理されません。これはホストの列挙には影響しません。これらを管理するためにカードをペアにする必要があります。カードをペアにするには、[パーティション デフォルトのリセット（Reset Partition Defaults）] または [カード設定の同期（Synchronize Card Configuration）] オプションを使用します。

FlexFlash でのシングル カード ミラーリングからデュアル カード ミラーリングへのアップグレード

次のいずれかの方法で、FlexFlash を使用したシングル カード ミラーリングからデュアル カード ミラーリングにアップグレードできます。

- サーバに空の FlexFlash カードを追加し、最新バージョンにファームウェアをアップグレードします。
- FlexFlash ファームウェアを最新バージョンにアップグレードした後、空のカードをサーバに追加します。

このいずれかの方法を使用する前に、次のガイドラインを考慮してください。

- RAID1 ミラーリングを作成するには、サーバに追加される空のカードのサイズが、サーバ上の既存のカードと正確に同じである必要があります。RAID1 ミラーリングをセットアップするうえで、同じカード サイズは必須事項です。
- ハイパーバイザ パーティション内の有効なデータを持つカードが、プライマリ正常カードとしてマークされていることを確認してください。Cisco IMC GUI または Cisco IMC CLI でこの状態を判別できます。カードの状態をプライマリ正常としてマークするには、Cisco IMC GUI の [設定情報のリセット（Reset Configuration）] オプションを使用するか、Cisco IMC CLI で **reset-config** コマンドを実行します。特定のカードの設定をリセットすると、セカンダリ カードはセカンダリ アクティブ非正常としてマークされます。
- RAID 正常性「Degraded」状態である場合、すべての読み取りおよび書き込みトランザクションは正常なカードで実行されます。このシナリオでは、データのミラーリングは行われません。データのミラーリングは、正常な RAID 状態の場合にのみ行われます。
- データのミラーリングは RAID パーティションにのみ適用されます。C シリーズ サーバでは、RAID モードでハイパーバイザ パーティションだけが動作します。
- 旧バージョンで使用するよう SD カードを設定していない場合、最新バージョンにアップグレードすると最新の 253 ファームウェアがロードされ、4 個のパーティションすべてがホストに列挙されます。

FlexFlash バージョンのアップグレード中に次のエラー メッセージが表示される場合があります。

```
Unable to communicate with Flexible Flash controller: operation ffCardsGet, status
CY_AS_ERROR_INVALID_RESPONSE”
```

さらに、カード ステータスが [不明（missing）] と示されることもあります。このエラーが発生する原因は、1.4(x) などの代替リリースまたは旧バージョンに意図せず切替えたためです。この場合、最新バージョンに戻すか、元の FlexFlash 1.4(x) 設定に切り替えることができます。最新の Cisco IMC バージョンに戻すことを選択した場合、Cisco FlexFlash 設定はそのまま残ります。旧バージョンの設定に切り替えることを選択した場合は、Flexflash 設定をリセットする必要があります。その場合、次の点に注意する必要があります。

- 複数のカードが存在する状態で旧バージョンに戻すと、2 番目のカードを検出したり管理したりすることはできません。
- カード タイプが SD253 である場合、Cisco IMC CLI から **reset-config** コマンドを 2 回実行する必要があります。1 回目は古いファームウェアをコントローラに再ロードして SD253 から SD247 タイプに移行し、2 回目の実行では列挙を開始します。

Flexible Flash コントローラ プロパティの設定

Cisco IMC の最新バージョンにアップグレードするか、以前のバージョンにダウングレードしてから設定をリセットすると、サーバは HV パーティションだけにアクセスします。

はじめる前に

- このタスクを実行するには、admin 権限でログインする必要があります。
- お使いのプラットフォームで Cisco Flexible Flash がサポートされている必要があります。

（注） このタスクを実行すると、ホストですべての仮想ドライブが再スキャンされるため、仮想ドライブに接続できなくなります。仮想ドライブを使用する前に Cisco Flexible Flash コントローラのプロパティを設定するか、このタスクを開始する前にホストの電源を切ることをお勧めします。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ストレージ（Storage）] タブをクリックします。

ステップ 2 [ストレージ（Storage）] タブの [Cisco FlexFlash] をクリックします。

ステップ 3 [コントローラ情報（Controller Info）] タブの [運用プロファイルの設定（Configure Operational Profile）] をクリックします。

ステップ 4 [運用プロファイル（Operational Profile）] ダイアログボックスで、次のフィールドを更新します。

表 *7*：*M5* サーバの操作プロファイル フィールド

名称	説明
[コントローラ（Controller）] フィールド	選択された Cisco Flexible Flash コントローラのシステム定義名。 この名前は変更できません。
[ファームウェアの動作モード（Firmware Operating Mode）] フィールド	システムによって表示されるメッセージ。ファームウェアの動作モードがミラーとして表示されます。
[スロット 1 読み取りエラーしきい値（SLOT-1 Read Error Threshold）] フィールド	Cisco Flexible Flash カードのスロット 1 へのアクセス中に許容される読み取りエラーの数。読み取りエラーの数がカード上のこのしきい値を超えると、カードが正常でないとマークされます。 読み取りエラーのしきい値を指定するには、1 ～ 255 の整数を入力します。検出されたエラー数に関係なく、カードがディセーブルにならないように指定するには、0（ゼロ）を入力します。

名称	説明
[スロット 1 書き込みエラーしきい値（SLOT-1 Write Error Threshold）] フィールド	Cisco Flexible Flash カードのスロット 1 へのアクセス中に許容される書き込みエラーの数。書き込みエラーの数がカード上のこのしきい値を超えると、カードが正常でないとマークされます。 書き込みエラーのしきい値を指定するには、1 ～ 255 の整数を入力します。検出されたエラー数に関係なく、カードがディセーブルにならないように指定するには、0（ゼロ）を入力します。

ステップ 5 [保存（Save）] をクリックします。

Flexible Flash コントローラ カードの設定

はじめる前に

- このタスクを実行するには、admin 権限でログインする必要があります。
- お使いのプラットフォームで Cisco Flexible Flash がサポートされている必要があります。

（注） このタスクを実行すると、ホストですべての仮想ドライブが再スキャンされるため、仮想ドライブに接続できなくなります。仮想ドライブを使用する前に Cisco Flexible Flash コントローラのプロパティを設定するか、このタスクを開始する前にホストの電源を切ることをお勧めします。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ストレージ（Storage）] タブをクリックします。

ステップ 2 [ストレージ（Storage）] タブの [Cisco FlexFlash] をクリックします。

ステップ 3 [アクション（Actions）] 領域で、[カードの設定（Configure Cards）] をクリックします。
[カードの設定（Configure Cards）] ダイアログボックスが表示されます。

ステップ 4 [カードの設定（Configure Cards）] ダイアログボックスで、次のフィールドを更新します。

名称	説明
[Mode] フィールド	モード タイプをミラーとして表示します。

名称	説明
[ミラー パーティション名（Mirror Partition Name）] フィールド	パーティションに割り当てる名前。
[自動同期（Auto Sync）] 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、選択したプライマリ カードからのデータが自動的にセカンダリ カードと同期されます。 （注） • このオプションを選択するには、カードが 2 枚必要です。 • このオプションを選択すると、セカンダリ カードのデータは消去され、プライマリ カードのデータで上書きされます。 • このステータスは、[仮想ドライブ（Virtual Drive）] タブに表示されます。
[プライマリ カードの選択（Select Primary Card）] ドロップダウン	プライマリ カードとして設定するスロット。次のいずれかになります。 • Slot1 • Slot2
[仮想ドライブ（Virtual Drive）] ドロップダウン	仮想ドライブのタイプ。次のいずれかになります。 • Removable • 削除不可能（Non Removable）

ステップ 5 [保存（Save）] をクリックします。

カードが選択したモードで設定されます。

Flexible Flash コントローラのリセット

通常の操作では、Cisco Flexible Flash のリセットが必要になることはありません。テクニカル サポートの担当者から明確に指示された場合にだけ、この手順を実行することを推奨します。

（注） この操作は、Cisco Flexible Flash コントローラ上の仮想ドライブへのトラフィックを中断させます。

はじめる前に

- このタスクを実行するには、admin 権限でログインする必要があります。
- お使いのプラットフォームで Cisco Flexible Flash がサポートされている必要があります。

手順

ステップ 1 タブの [Cisco FlexFlash] をクリックします。

ステップ 2 [Cisco FlexFlash] ペインの [コントローラ情報（Controller Info）] タブをクリックします。

ステップ 3 [アクション（Actions）] 領域で [FlexFlash コントローラのリセット（Reset FlexFlash Controller）] をクリックします。

ステップ 4 [OK] をクリックして確認します。

仮想ドライブの有効化

はじめる前に

- このタスクを実行するには、admin 権限でログインする必要があります。
- お使いのプラットフォームで Cisco Flexible Flash がサポートされている必要があります。

（注） このタスクを実行すると、ホストですべての仮想ドライブが再スキャンされるため、仮想ドライブに接続できなくなります。仮想ドライブを使用する前に Cisco Flexible Flash コントローラのプロパティを設定することをお勧めします。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ストレージ（Storage）] タブをクリックします。

ステップ 2 [ストレージ（Storage）] タブの [Cisco FlexFlash] をクリックします。

ステップ 3 [仮想ドライブ情報（Virtual Drive Info）] タブをクリックします。

ステップ 4 [仮想ドライブ情報（Virtual Drive Info）] タブで、[仮想ドライブの有効化/無効化（Enable/Disable Virtual Drive(s)）] をクリックします。

ステップ 5 [VD の有効化/無効化（Enable/Disable VD(s)）] ダイアログボックスで、有効にする仮想ドライブを選択します。

ステップ 6 [保存（Save）] をクリックします。
選択した仮想ドライブがホストで有効になります。

仮想ドライブの消去

はじめる前に

- このタスクを実行するには、admin 権限でログインする必要があります。
- お使いのプラットフォームで Cisco Flexible Flash がサポートされている必要があります。

（注） このタスクを実行すると、ホストですべての仮想ドライブが再スキャンされるため、仮想ドライブに接続できなくなります。仮想ドライブを使用する前に Cisco Flexible Flash コントローラのプロパティを設定することをお勧めします。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ストレージ（Storage）] タブをクリックします。

ステップ 2 [ストレージ（Storage）] タブの [Cisco FlexFlash] をクリックします。

ステップ 3 [仮想ドライブ情報（Virtual Drive Info）] タブをクリックします。

ステップ 4 [仮想ドライブ情報（Virtual Drive Info）] タブで、[仮想ドライブの消去（Erase Virtual Drive(s)）] をクリックします。

ステップ 5 [仮想ドライブの消去（Erase Virtual Drive(s)）] ダイアログボックスで、消去する仮想ドライブを選択します。

ステップ 6 [保存（Save）] をクリックします。
選択した仮想ドライブのデータが消去されます。

仮想ドライブの同期

はじめる前に

- このタスクを実行するには、admin 権限でログインする必要があります。
- お使いのプラットフォームで Cisco Flexible Flash がサポートされている必要があります。
- カードはミラー モードにする必要があります。

（注） このタスクを実行すると、ホストですべての仮想ドライブが再スキャンされるため、仮想ドライブに接続できなくなります。仮想ドライブを使用する前に Cisco Flexible Flash コントローラのプロパティを設定することをお勧めします。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ストレージ（Storage）] タブをクリックします。

ステップ 2 [ストレージ（Storage）] タブの [Cisco FlexFlash] をクリックします。

ステップ 3 [仮想ドライブ情報（Virtual Drive Info）] タブをクリックします。

ステップ 4 [仮想ドライブ情報（Virtual Drive Info）] タブで、[仮想ドライブの同期（Sync Virtual Drive）] をクリックします。

ステップ 5 確認ダイアログボックスで [OK] をクリックします。
仮想ドライブのハイパーバイザをプライマリ カードと同期させます。

FlexFlash ログの詳細の表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで [Cisco Flexible Flashコントローラ（Cisco Flexible Flash Controller）] をクリックします。

ステップ 3 [FlexFlashログ（FlexFlash Logs）] タブの [FlexFlashログテーブル（FlexFlash LogTable）] 領域で、次のフィールドを確認します。

[名前（Name）]	説明
[時刻（Time）] カラム	イベントが発生した日時。

[名前（Name）]	説明
[重大度（Severity）] カラム	イベントの重大度。次のいずれかになります。 • 緊急（Emergency） • アラート（Alert） • クリティカル（Critical） • エラー（Error） • 警告 • 情報（Info） • 通知（Notice） • デバッグ（Debug）
[説明（Description）] カラム	イベントの説明。

ステップ 4 [FlexFlashログ（FlexFlash Logs）] タブの [アクション（Actions）] 領域で、次のフィールドを確認します。

[名前（Name）]	説明
[表示（Show）] ドロップダウン リスト	フィルタを使用して Cisco IMC ログ エントリを表示する方法をカスタマイズします。これらの内容は次のとおりです。 • [クイック フィルタ（Quick Filter）]：デフォルト ビュー。 • [高度なフィルタ（Advanced Filter）]：1 つ以上の条件に基づいてログ エントリを表示するフィルタ オプション。マッチング ルールを使用して、[フィルタ（Filter）] フィールドで指定したルールのすべてまたはいくつかのルールの組み合わせと一致するエントリを表示できます。 新しいフィルタ条件を追加するには、[+] をクリックします。 設定したフィルタ条件に一致するエントリを表示するには、[移動（Go）] をクリックします。 設定したフィルタ条件を保存するには、[保存（Save）] アイコンをクリックします。これはユーザ定義のフィルタになり、後で使用できます。 （注） ユーザ定義のフィルタは [プリセット フィルタの管理（Manage Preset Filters）] ダイアログボックスに表示されます。 • [すべて（All）]：すべてのエントリが表示されます。 • [プリセット フィルタの管理（Manage Preset Filters）]：ユーザ定義のフィルタが表示されます。このダイアログボックスからユーザ定義のフィルタを編集または削除できます。 • [事前定義されたフィルタのリスト（List of pre-defined filters）]：システム定義のフィルタが表示されます。
[フィルタ（Filter）] アイコン	クイック フィルタ フィールドを表示または非表示にします。

[名前（Name）]	説明
[列（Column）] ドロップダウン リスト	表示する列を選択できます。

ステップ 5 [FlexFlashログ（FlexFlash Logs）] タブの [ログナビゲーションツールバー（Log Navigation Toolbar）] 領域で、次のフィールドを確認します。

[名前（Name）]	説明
<< 最も新しい（<<Newest）	イベントが 1 ページに入りきらない場合、このリンクをクリックすると最新のエントリが表示されます。 表示されるエントリの合計数は [1 ページあたりのエントリ数（Entries per Page）] ドロップダウン リストの設定によって異なります。
< 新しい（<Newer）	イベントが 1 ページに入りきらない場合、このリンクをクリックすると次ページが表示され、現在表示されているエントリより新しいエントリを確認できます。
[ログ エントリ（Log Entries）] フィールド	このフィールドは、表に現在表示されているのがどのログエントリなのかを示します。
より古い >（Older>）	イベントが 1 ページに入りきらない場合、このリンクをクリックすると次ページが表示され、現在表示されているエントリより古いエントリを確認できます。
最も古い >>（Oldest>>）	イベントが 1 ページに入りきらない場合、このリンクをクリックすると最も古いエントリが表示されます。
[ページ番号（Page Number）] ドロップダウン リスト	特定のページに移動できます。ドロップダウン リストからページ番号を選択します。
[行数（Number of Rows）] フィールド	現在のページに表示されている行数が表示されます。

FlexUtil コントローラの管理

C シリーズ M5 ラックマウント サーバは、サーバ ソフトウェア ツールおよびユーティリティのストレージ用に microSD メモリ カードをサポートします。ライザー 1 にはこの microSD メモリ カード スロットがあります。Cisco FlexUtil は、32 GB の microSD カードのみをサポートします。

次のユーザ認識可能なパーティションが microSD カードに存在します。

- Server Configuration Utility（SCU）–1.25 GB
- 診断-0.25 GB
- Host Update Utility（HUU）–1.5 GB
- ドライバ–8 GB
- ユーザ（User）

（注） MicroSD の各パーティションの数とサイズは固定されています。

いつでも、ホストに 2 つのパーティションをマップできます。（ユーザ パーティションを除く）これらのパーティションは、CIFS または NFS 共有により更新できます。第 2 レベルの BIOS ブート順序のサポートは、すべての起動可能なパーティションにも使用できます。

（注） ユーザ パーティションはストレージにのみ使用する必要があります。

FlexUtil コントローラのプロパティの設定

はじめる前に

このタスクを実行するには、admin 権限で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 [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで [Cisco FlexUtil Controller] をクリックします。

ステップ 3 [一般（General）] タブの [操作（Actions）] 領域で、[運用プロファイルの設定（Configure Operational Profile）] をクリックします。

ステップ 4 [運用プロファイル（Operational 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（Name）]	説明
[コントローラ（Controller）] フィールド	選択された Flex Util コントローラのシステム定義名。 この名前は変更できません。

[名前（Name）]	説明
[読み取りエラーしきい値（Read Error Threshold）] フィールド	Flex Util カードへのアクセス時の読み取りエラーの許容数。読み取りエラーの数がカード上のこのしきい値を超えると、カードが正常でないとマークされます。 読み取りエラーのしきい値を指定するには、1 ～ 255 の整数を入力します。検出されたエラー数に関係なく、カードがディセーブルにならないように指定するには、0（ゼロ）を入力します。
[書き込みエラーしきい値（Write Error Threshold）] フィールド	Flex Util カードへのアクセス時の書き込みエラーの許容数。書き込みエラーの数がカード上のこのしきい値を超えると、カードが正常でないとマークされます。 書き込みエラーのしきい値を指定するには、1 ～ 255 の整数を入力します。検出されたエラー数に関係なく、カードがディセーブルにならないように指定するには、0（ゼロ）を入力します。

FlexUtil カード設定のリセット

はじめる前に

このタスクを実行するには、admin 権限で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 [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで [Cisco FlexUtil Controller] をクリックします。

ステップ 3 [一般（General）] タブの [操作（Actions）] 領域で、[カード設定のリセット（Reset Card Configuration）] をクリックします。
このアクションは、FlexUtil カードの設定をデフォルトの設定にリセットします。

Cisco FlexUtil コントローラのプロパティの表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで [Cisco FlexUtil Controller] をクリックします。

ステップ 3 [一般（General）] タブの [一般（General）] 領域で、次のフィールドを確認します。

名称	説明
[製品名（Product Name）] フィールド	製品の名前。
[コントローラ名（Controller Name）] フィールド	コントローラの名前。
[コントローラ ステータス（Controller Status）] フィールド	FlexUtil カードの現在のステータス。次のいずれかになります。 • カードが存在しません • カードに異常があります • メタデータ読み取りエラー（Metadata Read Error） • カード アクセス エラー • 無効なカード サイズ（Invalid Card size） • メタデータが障害発生状態です • パーティションがありません。リセットが必要です • 無効なパーティションです。リセットが必要です • カードが書き込み禁止です

名称	説明
[Internal State] フィールド	コントローラの内部ステート。次のいずれかになります。 • [未初期化（Uninitialized）]：FlexUtil モニタリングが初期化されていません。 • [初期化中（Initializing）]：FlexUtil モニタリングが初期化中です。 • [設定中（Configuring）]：コントローラは FlexUtil カードの設定を確認しています。 • [OK]：FlexUtil カードはホストに接続されていません。 • [Connecting]：コントローラはホストに接続しようとしています。 • [Connected]：コントローラはホストに接続されています。 • [Failed]：コントローラに障害が発生しました。 詳細については、[Controller Status] フィールドを参照してください。 • [削除中（Erasing）]：FlexUtil カードを削除しています。 • [更新中（Updating）]：FlexUtil カードを更新しています。 • [リセット中（Resetting）]：カードの設定がリセットされます。

ステップ 4 [一般（General）] タブの [物理ドライブ数（Physical Drive Count）] 領域で、次のフィールドを確認します。

名称	説明
[Physical Drive Count] フィールド	サーバで検出された FlexUtil カードの数。

ステップ 5 [一般（General）] タブの [仮想ドライブ数（Virtual Drive Count）] 領域で、次のフィールドを確認します。

名称	説明
[仮想ドライブ数（Virtual Drive Count）] フィールド	サーバに搭載された FlexUtil カード上で設定されている仮想ドライブの数。

物理ドライブのプロパティの表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで [Cisco FlexUtil Controller] をクリックします。

ステップ 3 [物理ドライブ（Physical Drive）] タブの [一般（General）] 領域で、次のフィールドを確認します。

名称	説明
ドライブ	デバイスの名前。
ドライブ ステータス（Drive Status）	ドライブが存在するかどうかを示します。
[シリアル番号（Serial Number）] フィールド	FlexUtil カードのシリアル番号。
[Manufacturer ID] フィールド	FlexUtil カードの製造業者 ID。
[OEM ID] フィールド	FlexUtil カードの OEM ID（該当する場合）。
[製品名（Product Name）] フィールド	FlexUtil カードの名前。
[Product Revision] フィールド	FlexUtil カードのリビジョン番号。
[Manufacturing Date] フィールド	FlexUtil カードが製造された日付（mm/yy 形式）。
[Write Enabled] フィールド	このフィールドに [true] と表示されている場合、FlexUtil カードで書き込みが受け入れられます。
[ブロック サイズ（Block Size）] フィールド	FlexUtil カード上のブロック サイズ（バイト単位）。
[容量（Capacity）] フィールド	FlexUtil カードの容量（メガバイト単位）。

名称	説明
ヘルス（Health）	次のいずれかになります。 • 正常 • 異常（Unhealthy）

ステップ 4 [物理ドライブ（Physical Drive）] タブの [エラーカウンタ（Error Counters）] 領域で、次のフィールドを確認します。

名称	説明
[読み取りエラーしきい値（Read Error Threshold）] フィールド	FlexUtil カードへのアクセス時の読み取りエラーの許容数。
[読み取りエラー カウント（Read Error Count）] フィールド	FlexUtil カードが最初にインストールされてから現在までに I/O トラフィックの処理中に発生した読み取りエラーの数。
[書き込みエラーしきい値（Write Error Threshold）] フィールド	FlexUtil カードへのアクセス時の書き込みエラーの許容数。
[書き込みエラー カウント（Write Error Count）] フィールド	FlexUtil カードが最初にインストールされてから現在までに I/O トラフィックの処理中に発生した書き込みエラーの数。

ステップ 5 [物理ドライブ（Physical Drive）] タブの [パーティション（Partition）] 領域で、次のフィールドを確認します。

名称	説明
[パーティション カウント（Partition Count）] フィールド	FlexUtil カード上のパーティションの数。
[ドライブ有効（Drives Enabled）] フィールド	FlexUtil カード上のアクセスが有効になっている仮想ドライブ。

仮想ドライブのプロパティの表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで [Cisco FlexUtil Controller] をクリックします。

ステップ 3 [物理ドライブ（Physical Drive）] タブの [仮想ドライブ（Virtual Drives）] 領域で、次のフィールドを確認します。

名称	説明
[Virtual Drive] カラム	仮想ドライブの名前。
[ID] カラム	仮想ドライブ ID。
LUN ID	LUN ID（使用可能な場合）。
[ドライブ スコープ（Drive Scope）] 列	仮想ドライブがどのように設定されているか。これは常に [非RAID（NON RAID）] になります。
[サイズ（Size）] カラム	仮想ドライブのサイズ（MB 単位）。
[ドライブ ステータス（Drive Status）] 列	デバイスの状態。次のいずれかになります。 • 正常 • 異常（Unhealthy）
[Host Accessible] カラム	仮想ドライブがホストにマップされているかどうかを示します。次のいずれかになります。 • 接続されている状態 • 未接続 このフィールドに [接続中（connected）] と表示される場合、仮想ドライブがホストにマップされていることを意味します。
[ドライブ タイプ（Drive Type）] 列	ドライブのタイプ。これは常に [削除可能（Removable）] になります。

名称	説明
[進行中の操作（Operation in Progress）] 列	進行中の操作。次のいずれかになります。 • 削除中（Erasing） • 削除保留中（Erase-Pending） • 更新 • 更新保留中（Update-Pending） • NA （注） 何らかの操作の実行中にCisco IMC を再起動すると、その操作は中断され再起動後に操作の状態は NA に設定されます。
[最後の操作ステータス（Last Operation Status）] 列	直前の操作の状態。次のいずれかになります。 • 削除成功（Erase-Success） • 削除失敗（Erase-Failed） • 更新成功（Update-Success） • 更新失敗（Update-Failed）

ステップ 4 [物理ドライブ（Physical Drive）] タブの [アクション（Actions）] 領域で、次のフィールドを確認します。

名称	説明
仮想ドライブを有効/無効にします	仮想ドライブを有効/無効にできます。
仮想ドライブの消去（Erase Virtual Drive(s)）	仮想ドライブを FAT 32 形式にフォーマットできます。 （注） 進行中の消去操作または保留中の消去操作を取り消すことはできません。
画像の追加（Add Image）	SCU、HUU、診断、およびドライバの ISO イメージの設定を追加できます。

名称	説明
イメージの更新	仮想ドライブをISOイメージで更新できます。 （注） • 任意の仮想ドライブで削除または更新が進行中または保留状態の時は、[仮想（Virtual）] タブで使用可能ないずれのアクションも実行できません。 • 進行中の更新処理をキャンセルするには、[更新のキャンセル（Cancel Update）] ボタンを使用します。
更新のキャンセル（Cancel Update）	進行中の更新処理を取り消します。
イメージのマップ解除（Unmap Image）	ISO イメージの設定を削除できます。

仮想ドライブへのイメージのマッピング

はじめる前に

このタスクを実行するには、admin 権限で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 [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで [Cisco FlexUtil Controller] をクリックします。

ステップ 3 [仮想ドライブ（Virtual Drives）] タブをクリックします。

ステップ 4 [仮想ドライブ（Virtual Drives）] 領域で、仮想ドライブを選択して、[イメージの追加（Add Image）] をクリックします。

ステップ 5 [新しいイメージの追加（Add New Image）] ダイアログボックスで、次のフィールドを更新します。

名称	説明
[ボリューム（Volume）] フィールド	マッピング用にマウントされるイメージの ID。次のいずれかになります。 • SCU • 診断 • HUU • 購入要因
[マウント タイプ（Mount Type）] ドロップダウン リスト	The type of mapping.次のいずれかになります。 • [NFS]：ネットワーク ファイル システム。 • [CIFS]：Common Internet File System。 • [WWW(HTTP/HTTPS)]：HTTP ベースまたは HTTPS ベースのシステム。
[リモート共有（Remote Share）] フィールド	マップするイメージの URL。形式は、選択した [マウント タイプ（Mount Type）] によって異なります。 • [NFS]：serverip:/share path を使用します。 • [CIFS]：//serverip/share path を使用します。 • [WWW(HTTP/HTTPS)]：http[s]://serverip/share を使用します。
[リモート ファイル（Remote File）] フィールド	リモート共有の .iso ファイルの名前と場所。次に、リモート共有ファイルの例を示します。 • [NFS]：/softwares/ucs-cxx-scu-3.1.9.iso • [CIFS]：/softwares/ucs-cxx-scu-3.1.9.iso • [WWW(HTTP/HTTPS)]：http[s]://softwares/ucs-cxx-scu-3.1.9.iso

名称	説明
[マウント オプション（Mount Options）] フィールド	カンマ区切りリストで入力される業界標準のマウント オプション。オプションは選択された [マウント タイプ（Mount Type）] によって異なります。 [NFS] を使用している場合は、このフィールドを空白のままにするか、次の中から 1 つ以上を入力します。 • ro • rw • nolock • noexec • soft • port=VALUE • timeo=VALUE • retry=VALUE [CIFS] を使用している場合は、このフィールドを空白のままにするか、次の中から 1 つ以上を入力します。 • soft • nounix • noserverino [WWW(HTTP/HTTPS)] を使用している場合は、このフィールドを空白のままにするか、次を入力します。 • noauto （注） イメージをマウントする前に、Cisco IMC はサーバに ping を実行することによって、エンド サーバへの到達可能性の確認を試みます。 • username=VALUE • password=VALUE

ステップ 6 省略可能：[イメージの追加（Add Image）] ボタンはトグル ボタンです。イメージをマップした後、ドライブから同じイメージを解除する場合は、仮想ドライブを選択して [イメージのマップ解除（Unmap Image）] をクリックします。

仮想ドライブ上のイメージの更新

はじめる前に

このタスクを実行するには、admin 権限で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 [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで [Cisco FlexUtil Controller] をクリックします。

ステップ 3 [仮想ドライブ（Virtual Drives）] タブをクリックします。

ステップ 4 [仮想ドライブ（Virtual Drives）] 領域で、イメージを更新する仮想ドライブを選択し、[イメージの更新（Update Image）] をクリックします。

ステップ 5 省略可能：実行中の更新操作をキャンセルする場合は、[更新のキャンセル（Cancel Update）] をクリックします。

仮想ドライブからのイメージのマッピング解除

はじめる前に

このタスクを実行するには、admin 権限で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 [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで [Cisco FlexUtil Controller] をクリックします。

ステップ 3 [仮想ドライブ（Virtual Drives）] タブをクリックします。

ステップ 4 [仮想ドライブ（Virtual Drives）] 領域で、イメージを削除する仮想ドライブを選択し、[イメージのマップ解除（Unmap Image）] をクリックします。

仮想ドライブの消去

はじめる前に

このタスクを実行するには、admin 権限で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 [ストレージ（Storage）] メニューをクリックします。

ステップ 2 [ストレージ（Storage）] メニューで [Cisco FlexUtil Controller] をクリックします。

ステップ 3 [仮想ドライブ（Virtual Drives）] タブをクリックします。

ステップ 4 [仮想ドライブ（Virtual Drives）] 領域で、削除する仮想ドライブを選択して、[仮想ドライブの削除（Erase Virtual Drive）] をクリックします。

第 13 章

コミュニケーション サービスの設定

この章の内容は、次のとおりです。

HTTP の設定

はじめる前に

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 [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [通信サービス（Communication Services）] をクリックします。

ステップ 3 [HTTP プロパティ（HTTP Properties）] 領域で、次のプロパティを更新します。

[名前（Name）]	説明
[HTTP/S 有効（HTTP/S Enabled）] チェックボックス	HTTP および HTTPS が Cisco IMC でイネーブルかどうか。

[名前（Name）]	説明
[HTTP の HTTPS へのリダイレクトを有効（Redirect HTTP to HTTPS Enabled）] チェックボックス	イネーブルの場合、HTTP 経由で試行される通信はすべて同等の HTTPS アドレスにリダイレクトされます。 HTTP をイネーブルにしている場合は、このオプションをイネーブルにすることを強く推奨します。
[HTTP ポート（HTTP Port）] フィールド	HTTP 通信に使用するポート。デフォルトは 80 です。
[HTTPS ポート（HTTPS Port）] フィールド	HTTPS 通信に使用するポート。デフォルトは 443 です。
[セッション タイムアウト（Session Timeout）] フィールド	HTTP 要求の間、Cisco IMC がタイム アウトしてセッションを終了するまで待機する秒数。 60 ～ 10,800 の整数を入力します。デフォルトは 1,800 秒です。
[最大セッション数（Max Sessions）] フィールド	Cisco IMC で許可されている HTTP および HTTPS の同時セッションの最大数。 この値は変更できません。
[アクティブなセッション（Active Sessions）] フィールド	Cisco IMC で現在実行されている HTTP および HTTPS セッションの数。

ステップ 4 [変更の保存（Save Changes）] をクリックします。

Configuring SSH

はじめる前に

SSH 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 [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [通信サービス（Communication Services）] をクリックします。

ステップ 3 [SSH プロパティ（SSH Properties）] 領域で、次のプロパティを更新します。

[名前（Name）]	説明
[SSH 有効（SSH Enabled）] チェックボックス	SSH が Cisco IMC でイネーブルかどうか。
[SSH ポート（SSH Port）] フィールド	セキュア シェル アクセスに使用するポート。デフォルト値は 22 です。
[SSH タイムアウト（SSH Timeout）] フィールド	SSH 要求がタイムアウトしたものとシステムが判断するまで待機する秒数。 60 ～ 10,800 の整数を入力します。デフォルトは 1,800 秒です。
[最大セッション数（Max Sessions）] フィールド	Cisco IMC で許可されている SSH の同時セッションの最大数。 この値は変更できません。
[アクティブなセッション（Active Sessions）] フィールド	現在 Cisco IMC で実行されている SSH セッションの数。

ステップ 4 [変更の保存（Save Changes）] をクリックします。

XML API の設定

Cisco IMC 用の XML API

Cisco Cisco IMC XML アプリケーション プログラミング インターフェイス（API）は、C シリーズ ラックマウント サーバ用の Cisco IMC に対するプログラマチック インターフェイスです。この API は、HTTP または HTTPS 経由で XML ドキュメントを受け取ります。

XML API の詳細については、『*Cisco UCS Rack-Mount Servers Cisco IMC XML API Programmer's Guide*』を参照してください。

XML API のイネーブル化

はじめる前に

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 [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [通信サービス（Communication Services）] をクリックします。

ステップ 3 [XML API プロパティ（XML API Properties）] 領域で、次のプロパティを更新します。

[名前（Name）]	説明
[XML API 有効（XML API Enabled）] チェックボックス	このサーバで API アクセスが許可されているかどうか。
[最大セッション数（Max Sessions）] フィールド	Cisco IMC で許可されている API の同時セッションの最大数。 この値は変更できません。
[アクティブなセッション（Active Sessions）] フィールド	現在 Cisco IMC で実行されている API セッションの数。

ステップ 4 [変更の保存（Save Changes）] をクリックします。

Configuring IPMI

IPMI Over LAN

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）では、サーバプラットフォームに組み込まれているサービス プロセッサとのインターフェイスのためのプロトコルを定義しています。このサービスプロセッサはベースボード管理コントローラ（BMC）と呼ばれ、サーバのマザーボードに存在します。BMC は、メイン プロセッサおよびボード上の他の要素に、簡単なシリアル バスを使用してリンクします。

通常動作の間、IPMI は、サーバのオペレーティング システムがシステム ヘルスについての情報を取得し、システムのハードウェアを制御できるようにします。たとえば、IPMI を使用すると、温度、ファンの速度、および電圧などのセンサーをモニタして、問題を事前に検出できます。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、サーバのオペレーティング システムは BMC に対して、ファンの速度を上げたり、プロセッサの速度を下げたりして問題に対処するよう指示できます。

IPMI over LAN の設定

IPMI over LAN は、Cisco IMC を IPMI メッセージで管理する場合に設定します。

はじめる前に

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 [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [通信サービス（Communication Services）] をクリックします。

ステップ 3 [IPMI over LAN プロパティ（IPMI over LAN Properties）] 領域で、BMC 1、BMC 2、CMC 1、CMC 2 の次のプロパティを更新します。

[名前（Name）]	**説明**
[有効化（Enable）] チェックボックス	このサーバで IPMI アクセスが許可されているかどうか。
[特権レベルの制限（Privilege Level Limit）] ドロップダウンリスト	このサーバで IPMI セッションに割り当て可能な最高特権レベル。次のいずれかになります。 • [読み取り専用（read-only）] : IPMI ユーザは情報を表示できますが、変更することはできません。このオプションを選択した場合、「Administrator」、「Operator」、または「User」ユーザ ロールを持つ IPMI ユーザが作成できるのは、読み取り専用の IPMI セッションだけです。それ以外に所持している IPMI 特権は関係ありません。 • [ユーザ（user）] : IPMI ユーザはいくつかの機能を実行できますが、管理タスクは実行できません。このオプションを選択した場合、「Administrator」または「Operator」ユーザ ロールを持つ IPMI ユーザがこのサーバで作成できるのは、ユーザ セッションと読み取り専用セッションだけです。 • [管理者（admin）] : IPMI ユーザは使用可能なすべてのアクションを実行できます。このオプションを選択した場合、「Administrator」ユーザ ロールを持つ IPMI ユーザは、管理者、ユーザ、および読み取り専用セッションをこのサーバで作成できます。
[暗号化キー（Encryption Key）] フィールド	IPMI 通信に使用する IPMI 暗号キー。
[ランダム化（Randomize）] ボタン	IPMI 暗号化キーをランダムな値に変更できます。

ステップ 4 [変更の保存（Save Changes）] をクリックします。

Configuring SNMP

SNMP

Cisco UCS C シリーズ ラックマウント サーバ は、サーバの設定およびステータスを表示したり、SNMP トラップによって障害とアラートの情報を送信したりするために、簡易ネットワーク管理プロトコル（SNMP）をサポートしています。Cisco IMC でサポートされている管理情報ベース（MIB）ファイルの詳細については、次の URL にある『*MIB Quick Reference for Cisco UCS*』を参照してください。http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/sw/mib/b-series/b_UCS_MIBRef.html

SNMP プロパティの設定

はじめる前に

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 [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [通信サービス（Communication Services）] をクリックします。

ステップ 3 [コミュニケーション サービス（Communications Services）] ペインの [SNMP] タブをクリックします。

ステップ 4 [SNMP プロパティ（SNMP Properties）] 領域で、次のプロパティを更新します。

[名前（Name）]	説明
[SNMP 有効（SNMP Enabled）] チェックボックス	このサーバが指定のホストに SNMP トラップを送信するかどうか。 （注） このチェックボックスをオンにしたら、SNMP ユーザまたはトラップを設定する前に、[変更内容を保存（Save Changes）] をクリックする必要があります。

[名前（Name）]	説明
[SNMP ポート（SNMP Port）] フィールド	Cisco IMC SNMP エージェントが動作するポート。 1 ～ 65535 の範囲内の SNMP ポート番号を入力します。デフォルトのポート番号は 161 です。 （注） システム コールに予約済みのポート番号（たとえば 22、23、80、123、443、623、389、636、3268、3269、2068 など）は、SNMP ポートとして使用できません。
[アクセス コミュニティ ストリング（Access Community String）] フィールド	Cisco IMC が任意の SNMP に含めるデフォルトの SNMP v1 または v2c コミュニティ名により、動作が実行されます。 最大 18 文字の文字列を入力します。
[SNMP コミュニティ アクセス（SNMP Community Access）] ドロップダウン リスト	次のいずれかになります。 • [無効（Disabled）]：このオプションは、インベントリ テーブルの情報へのアクセスをブロックします。 • [制限付き（Limited）]：このオプションは、インベントリ テーブルの情報の読み取りアクセスを部分的に提供します。 • [フル（Full）]：このオプションは、インベントリ テーブルの情報の読み取りフル アクセスを提供します。 （注） SNMP コミュニティ アクセスは、SNMP v1 および v2c ユーザのみに適用されます。
[トラップ コミュニティ ストリング（Trap Community String）] フィールド	他のデバイスに SNMP トラップを送信するために使用される SNMP コミュニティ グループの名前。 最大 18 文字の文字列を入力します。 （注） このフィールドは、SNMP v1 および v2c ユーザのみに表示されます。SNMP v3 ユーザは、SNMP v3 クレデンシャルを使用する必要があります。
[システム連絡先（System Contact）] フィールド	SNMP の実装を担当するシステムの連絡先。 電子メール アドレスまたは名前と電話番号など、最大 64 文字の文字列を入力します。
[システム ロケーション（System Location）] フィールド	SNMP エージェント（サーバ）が動作するホストの場所。 最大 64 文字の文字列を入力します。
[SNMP 入力エンジン ID（SNMP Input Engine ID）] フィールド	ユーザ定義の一意の静的エンジン ID。

[名前（Name）]	説明
[SNMP エンジン ID（SNMP Engine ID）] フィールド	管理用デバイスを識別する一意の文字列。[SNMP 入力エンジン ID（SNMP Input Engine ID）] が定義されている場合は、その値から文字列が生成されます。そうでない場合は、BMC シリアル番号から派生します。

ステップ 5 [変更の保存（Save Changes）] をクリックします。

次の作業

SNMP トラップを設定します。

SNMP トラップ設定の指定

はじめる前に

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 [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [通信サービス（Communication Services）] をクリックします。

ステップ 3 [コミュニケーション サービス（Communications Services）] ペインの [SNMP] タブをクリックします。

ステップ 4 [トラップ宛先（Trap Destinations）] タブをクリックします。

ステップ 5 [トラップ宛先（Trap Destinations）] 領域で、次のいずれかを実行できます。

- テーブルから既存のユーザを選択し、[トラップの変更（Modify Trap）] をクリックします。
- 新しいユーザを作成するには、[トラップの追加（Add Trap）] をクリックします。

（注） フィールドが強調表示されていない場合は、[有効（Enabled）] を選択します。

ステップ 6 [トラップの詳細（Trap Details）] ダイアログボックスで、次のフィールドに値を入力します。

[名前（Name）]	説明
[ID] フィールド	トラップの宛先 ID。この値は変更できません。
[有効（Enabled）] チェックボックスドロップダウン リスト	オンにすると、このトラップがサーバでアクティブになります。

[名前（Name）]	説明
[バージョン（Version）] ドロップダウン リスト	トラップに使用される SNMP バージョンおよびモデル。次のいずれかになります。 • V2 • V3
[トラップ タイプ（Trap Type）] オプション ボタンドロップダウン リスト	送信するトラップのタイプ。次のいずれかになります。 • [トラップ（Trap）] : このオプションを選択すると、トラップが宛先に送信されますが、通知は受信しません。 • [伝達（Inform）] : V2 ユーザに対してのみこのオプションを選択できます。これを選択すると、宛先でトラップが受信されたときに通知を受け取ります。
[ユーザ（User）] ドロップダウン リスト	ドロップダウンリストに使用可能なすべてのユーザが表示されます。そのリストからユーザを選択します。
[トラップ宛先アドレス（Trap Destination Address）] フィールド	SNMP トラップ情報の送信先のアドレス。トラップの宛先として IPv4 または IPv6 アドレスまたはドメイン名を設定できます。
[ポート（Port）]	サーバがトラップの宛先との通信に使用するポート。 1 ～ 65535 の範囲内のトラップ宛先ポート番号を入力します。

ステップ 7 [変更の保存（Save Changes）] をクリックします。

ステップ 8 トラップの宛先を削除する場合は、行を選択し、[削除（Delete）] をクリックします。
削除の確認プロンプトで、[OK] をクリックします。

テスト SNMP トラップ メッセージの送信

はじめる前に

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 [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [通信サービス（Communication Services）] をクリックします。

ステップ 3 [通信サービス（Communication Services）] ペインの [SNMP] をクリックします。

ステップ 4 [トラップ宛先（Trap Destinations）] 領域で、目的の SNMP トラップ宛先の行を選択します。

ステップ 5 [SNMP テスト トラップの送信（Send SNMP Test Trap）] をクリックします。
SNMP テスト トラップ メッセージがトラップ宛先に送信されます。

（注） テスト メッセージを送信するために、トラップは設定済みで、イネーブルにされている必要があります。

SNMP ユーザの管理

はじめる前に

- 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。
- SNMP がイネーブルである必要があります。

手順

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

ステップ 2 [管理者（Admin）] メニューの [通信サービス（Communication Services）] をクリックします。

ステップ 3 [コミュニケーション サービス（Communications Services）] ペインの [SNMP] タブをクリックします。

ステップ 4 [ユーザ設定（User Settings）] 領域で、次のプロパティを更新します。

[名前（Name）]	説明
[ユーザの追加（Add User）] ボタン	テーブル内で使用できる行をクリックし、このボタンをクリックして新規の SNMP ユーザを追加します。
[ユーザの変更（Modify User）] ボタン	テーブル内で変更するユーザを選択し、このボタンをクリックして、選択した SNMP ユーザを変更します。
[ユーザの削除（Delete User）] ボタン	テーブル内で削除するユーザを選択し、このボタンをクリックして、選択した SNMP ユーザを削除します。
[ID] カラム	SNMP ユーザに対してシステムが割り当てる識別子。

[名前（Name）]	説明
[名前（Name）] カラム	SNMP ユーザ名。
[認証タイプ（Auth Type）] カラム	ユーザ認証タイプ。
[プライバシー タイプ（Privacy Type）] カラム	ユーザ プライバシー タイプ。

ステップ 5 [変更の保存（Save Changes）] をクリックします。

SNMP ユーザの設定

はじめる前に

- 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。
- SNMP がイネーブルである必要があります。

手順

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

ステップ 2 [管理者（Admin）] メニューの [通信サービス（Communication Services）] をクリックします。

ステップ 3 [コミュニケーション サービス（Communications Services）] ペインの [SNMP] タブをクリックします。

ステップ 4 [ユーザ設定（User Settings）] 領域で、次のいずれかの操作を実行します。

- テーブルから既存のユーザを選択し、[ユーザの変更（Modify User）] をクリックします。
- [ユーザ（Users）] 領域で行を選択し、[ユーザの追加（Add User）] をクリックして新しいユーザを作成します。

ステップ 5 [SNMP ユーザの詳細（SNMP User Details）] ダイアログボックスで、次のプロパティを更新します。

[名前（Name）]	説明
[ID] フィールド	ユーザの固有識別情報。このフィールドは変更できません。

[名前（Name）]	説明
[名前（Name）] フィールド	SNMP ユーザ名。 1 ～ 31 個の文字またはスペースを入力します。 （注） Cisco IMC は先頭または末尾のスペースを自動的に切り詰めます。
[セキュリティ レベル（Security Level）] ドロップダウン リスト	このユーザのセキュリティ レベル。次のいずれかになります。 • [no auth, no priv]：このユーザには、許可パスワードもプライバシー パスワードも不要です。 • [auth, no priv]：このユーザには、許可パスワードが必要ですが、プライバシー パスワードは不要です。このオプションを選択すると、Cisco IMC は後述の認証フィールドをイネーブルにします。 • [auth, priv]：このユーザには、許可パスワードとプライバシー パスワードの両方が必要です。このオプションを選択すると、Cisco IMC は認証フィールドおよびプライバシー フィールドをイネーブルにします。
[認証タイプ（Auth Type）] ドロップダウン	許可タイプ。次のいずれかになります。 • MD5 • SHA
[認証パスワード（Auth Password）] フィールド	この SNMP ユーザの許可パスワード。 8 ～ 64 個の文字またはスペースを入力します。 （注） Cisco IMC は先頭または末尾のスペースを自動的に切り詰めます。
[認証パスワードの確認（Confirm Auth Password）] フィールド	確認のための許可パスワードの再入力。
[プライバシー タイプ（Privacy Type）] ドロップダウン	プライバシー タイプ。次のいずれかになります。 • DES • AES
[プライバシー パスワード（Privacy Password）] フィールド	この SNMP ユーザのプライバシー パスワード。 8 ～ 64 個の文字またはスペースを入力します。 （注） Cisco IMC は先頭または末尾のスペースを自動的に切り詰めます。

[名前（Name）]	説明
[プライバシー パスワードの確認（Confirm Privacy Password）] フィールド	確認のための許可パスワードの再入力。

ステップ 6 [変更の保存（Save Changes）] をクリックします。

ステップ 7 ユーザを削除する場合は、ユーザを選択し、[ユーザの削除（Delete User）] をクリックします。削除の確認プロンプトで、[OK] をクリックします。

電子メール アラートを SMTP で送信するようにサーバを設定

Cisco IMC は、SNMP に依存せずに、電子メール ベースのサーバ障害通知を受信者に送信できます。システムは簡易メール転送プロトコル（SMTP）を使用して、設定されている SMTP サーバに電子メール アラートとしてサーバ障害を送信します。

最大 4 人の受信者に対応しています。

電子メール アラートの受信用に SMTP サーバを設定

サーバ障害に関するメール通知を受信できるように、SMTP のプロパティを設定し、[メール アラート（Mail Alert）] タブで電子メール受信者を追加します。

はじめる前に

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

ステップ 2 [管理者（Admin）] メニューの [通信サービス（Communication Services）] をクリックします。

ステップ 3 [コミュニケーション サービス（Communications Services）] ペインで、[メール アラート（Mail Alert）] タブをクリックします。

ステップ 4 [SMTP プロパティ（SMTP Properties）] 領域で、次のプロパティを更新します。

名称	説明
[SMTP の有効化（SMTP Enabled）] チェックボックス	オンにすると、SMTP サービスが有効になります。
[SMTP サーバアドレス（SMTP Server Address）] フィールド	SMTP サーバのアドレスを入力できます。
[SMTP ポート（SMTP Port）] フィールド	SMTP ポートの番号を入力できます。デフォルトのポート番号は 25 です。
[報告する最小重大度（Minimum Severity to Report）] ドロップダウン リスト	電子メール アラートを受信する最小重大度レベルを選択できます。次のいずれかになります。 • 条件 • 警告 • [マイナー（Minor）] • [メジャー（Major）] • クリティカル（Critical） 最小重大度レベルを選択すると、そのレベルとそれ以上のレベルに該当する場合にメール アラートが送信されます。たとえば、最小重大度レベルとして [マイナー（Minor）] を選択した場合は、マイナー、メジャー、およびクリティカルな障害イベントが発生したときに電子メール アラートを受信できます。

ステップ 5 [SMTP 受信者（SMTP Recipients）] 領域で、次の手順を実行します。

a) [追加 (+)（Add (+)）] ボタンをクリックし、通知の送信先となる電子メール受信者を追加します。メール ID を入力し、[保存（Save）] をクリックします。
電子メール受信者を削除するには、電子メール受信者を選択して [削除 (X)（Delete (X)）] ボタンをクリックします。

b) 追加した電子メール受信者に到達可能かどうかを確認するには、[テスト メールの送信（Send Test Mail）] をクリックします。
電子メール アドレスおよび SMTP の設定が有効な場合は、電子メールが送信されたことを示すメッセージが確認ポップアップ ウィンドウに表示されます。設定が無効な場合は、電子メールが送信されなかったことを示すメッセージが確認ポップアップ ウィンドウに表示されます。
[到達可能性（Reachability）] カラムは、電子メール受信者にテスト メールが正常に送信されたかどうかを示します。[到達可能性（Reachability）] カラムには次のいずれかの値が示されます。

- [はい（Yes）]（テスト メールが正常に送信された場合）
- [いいえ（No）]（テスト メールが正常に送信されなかった場合）

- [na]（テスト メールの送信が実行されなかった場合）

ステップ 6 [変更の保存（Save Changes）] をクリックします。

SMTP 電子メール受信者の追加

サーバ障害に関するメール通知を受信できるように、[メール アラート（Mail Alert）] タブで電子メール受信者を追加します。

はじめる前に

- 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。
- [SMTP プロパティ（SMTP Properties）] 領域で SMTP サーバのプロパティを設定します。参照先 電子メール アラートの受信用に SMTP サーバを設定, （315 ページ）

手順

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

ステップ 2 [管理者（Admin）] メニューの [通信サービス（Communication Services）] をクリックします。

ステップ 3 [コミュニケーション サービス（Communications Services）] ペインで、[メール アラート（Mail Alert）] タブをクリックします。

ステップ 4 [SMTP 受信者（SMTP Recipients）] 領域で、次の手順を実行します。

a) [追加 (+)（Add (+)）] ボタンをクリックし、通知の送信先となる電子メール受信者を追加します。メール ID を入力し、[保存（Save）] をクリックします。

b) 追加した電子メール受信者に到達可能かどうかを確認するには、[テスト メールの送信（Send Test Mail）] をクリックします。
電子メール アドレスおよび SMTP の設定が有効な場合は、電子メールが送信されたことを示すメッセージが確認ポップアップ ウィンドウに表示されます。設定が無効な場合は、電子メールが送信されなかったことを示すメッセージが確認ポップアップ ウィンドウに表示されます。
[到達可能性（Reachability）] カラムは、電子メール受信者にテスト メールが正常に送信されたかどうかを示します。[到達可能性（Reachability）] カラムには次のいずれかの値が示されます。

- [はい（Yes）]（テスト メールが正常に送信された場合）
- [いいえ（No）]（テスト メールが正常に送信されなかった場合）
- [na]（テスト メールの送信が実行されなかった場合）

第 14 章

証明書とサーバ セキュリティの管理

この章の内容は、次のとおりです。

サーバ証明書の管理

証明書署名要求（CSR）を生成して新しい証明書を取得し、新しい証明書を Cisco IMC にアップロードして現在のサーバ証明書と交換することができます。サーバ証明書は、Verisign のようなパブリック認証局（CA）、または独自に使用している認証局のいずれかによって署名されます。生成される証明書キーの長は 2048 ビットです。

（注） この章に記載されている以下のタスクを実行する前に、Cisco IMC の時刻が現在の時刻に設定されていることを確認します。

手順

ステップ 1 Cisco IMC から CSR を生成します。

ステップ 2 証明書の発行と署名を行う認証局に CSR ファイルを送信します。組織で独自の自己署名証明書を生成している場合は、CSR ファイルを使用して自己署名証明書を生成できます。

ステップ 3 新しい証明書を Cisco IMCにアップロードします。

（注） アップロードする証明書は、Cisco IMC によって生成された CSR から作成されたものでなければなりません。この方法で作成されていない証明書はアップロードしないでください。

証明書署名要求の生成

（注） [コモンネーム（Common Name）] および [組織単位（Organization Unit）] フィールドには特殊文字（たとえばアンパサンド（**&**））を使用しないでください。

はじめる前に

- 証明書を設定するには、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。
- Cisco IMC の時刻が現在の時刻に設定されていることを確認してください。

手順

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

ステップ 2 [管理者（Admin）] メニューの [セキュリティ管理（Security Management）] をクリックします。

ステップ 3 [アクション（Actions）] 領域で、[新しい証明書署名要求の生成（Generate New Certificate Signing Request）] リンクをクリックします。
[新しい証明書署名要求の生成（Generate New Certificate Signing Request）] ダイアログボックスが表示されます。

ステップ 4 [新しい証明書署名要求の生成（Generate New Certificate Signing Request）] ダイアログボックスで、次のプロパティを更新します。

[名前（Name）]	**説明**
[コモン ネーム（Common Name）] フィールド	Cisco IMC の完全修飾名。 デフォルトでは、サーバの CN は CXXX-YYYYYY 形式で表示されます（XXX はサーバのモデル番号で YYYYYY はシリアル番号です）。 最新バージョンにアップグレードすると、CN はそのまま保持されます。
[組織名（Organization Name）] フィールド	証明書を要求している組織。

[名前（Name）]	説明
[組織単位（Organization Unit）] フィールド	組織ユニット。
[地域（Locality）] フィールド	証明書を要求している会社の本社が存在する市または町。
[州/都道府県名（State Name）] フィールド	証明書を要求している会社の本社が存在する州または行政区分。
[国コード（Country Code）] ドロップダウン リスト	会社が存在する国。
[電子メール（Email）] フィールド	会社の電子メールの連絡先。
署名アルゴリズム（Signature Algorithm）	証明書署名要求の生成に使用する署名アルゴリズムを選択できます。次のいずれかになります。 • SHA384 • SHA1 • SHA256 • SHA512 証明書署名要求の生成に対してデフォルトで選択される署名アルゴリズムは SHA384 です。
[自己署名証明書（Self Signed Certificate）] チェックボックス	自己署名した証明書を生成します。 警告　証明書の生成が成功した後、Cisco IMC Web GUI が再起動します。管理コントローラとの通信が一時的に切断され、再ログインが必要な場合があります。 （注）　イネーブルの場合、CSR が生成され、自動的に署名およびアップロードが行われます。

（注）　自己署名証明書が有効な場合は、ステップ 5 および 6 を無視します。

ステップ 5　[CSR の作成（Generate CSR）] をクリックします。
[csr.txt を開く（Opening csr.txt）] ダイアログボックスが表示されます。

ステップ 6　CSR ファイル csr.txt を管理するには、次のいずれかの手順を実行します。

a) [プログラムから開く（Open With）] をクリックして csr.txt を表示します。
b) [ファイルを保存（Save File）] をクリックしてから [OK] をクリックし、ローカル マシンに csr.txt を保存します。

次の作業

- 証明書の発行と署名を行う認証局にCSRファイルを送信します。組織で独自の自己署名証明書を生成している場合は、CSR ファイルを使用して自己署名証明書を生成できます。
- 証明書のタイプが [サーバ（Server）] であることを確認します。

自己署名証明書の作成

パブリック認証局（CA）を使用してサーバ証明書の生成と署名を行う代わりに、独自の CA を運用して独自の証明書に署名することができます。このセクションでは、Linux で実行されている OpenSSL 証明書サーバを使用して CA を作成するコマンドおよびサーバ証明書を生成するコマンドについて説明します。OpenSSL の詳細については、http://www.openssl.orgを参照してください。

（注） これらのコマンドは、Cisco IMC ではなく、OpenSSL パッケージを使用している Linux サーバで入力します。

はじめる前に

- 組織内のサーバで、証明書サーバのソフトウェア パッケージを取得してインストールします。
- Cisco IMC の時刻が現在の時刻に設定されていることを確認してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**openssl genrsa -out** *CA_keyfilename keysize* 例： `# openssl genrsa -out ca.key 2048`	このコマンドは、CA で使用される RSA 秘密キーを生成します。 （注） ユーザ入力なしで CA がキーにアクセスできるように、このコマンドに -des3 オプションは使用しないでください。 指定されたファイル名には、指定されたサイズの RSA キーが含まれています。
ステップ 2	**openssl req -new -x509 -days** *numdays***-key** *CA_keyfilename***-out** *CA_certfilename* 例： `# openssl req -new -x509 -days 365 -key ca.key -out ca.crt`	このコマンドは、指定されたキーを使用して、CA の自己署名証明書を新規に作成します。証明書は指定された期間有効になります。このコマンドは、ユーザに証明書の追加情報を求めるプロンプトを表示します。 証明書サーバは、アクティブな CA です。

	コマンドまたはアクション	目的
ステップ 3	**echo "nsCertType = server" > openssl.conf** 例： `# echo "nsCertType = server" > openssl.conf`	このコマンドは、証明書がサーバ限定の証明書であることを指定する行を OpenSSL 設定ファイルに追加します。この指定により、認証されたクライアントがサーバになりすます man-in-the-middle 攻撃を防御できます。 OpenSSL 設定ファイル openssl.conf には、"nsCertType = server" という文が含まれています。
ステップ 4	**openssl x509 -req -days** *numdays*-**in** *CSR_filename*-**CA** *CA_certfilename*-**set_serial 04 -CAkey** *CA_keyfilename*-**out** *server_certfilename*-**extfile openssl.conf** 例： `# openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 04 -CAkey ca.key -out myserver05.crt -extfile openssl.conf`	このコマンドは、CA が CSR ファイルを使用してサーバ証明書を生成するように指示します。 サーバ証明書は、出力ファイルに含まれています。
ステップ 5	**openssl x509 -noout -text -purpose -in <cert file>** 例： `openssl x509 -noout -text -purpose -in <cert file>`	生成された証明書のタイプが [サーバ（Server）] であることを確認します。 （注） フィールド [サーバ SSL（Server SSL）] および [Netscape SSL] サーバの値が [はい（Yes）] でない場合は、タイプが [サーバ（Server）] の証明書を生成するように openssl.conf が設定されていることを確認します。
ステップ 6	生成された証明書に正しい使用期限が設定されていない場合は、Cisco IMC の時刻が現在の時刻に設定されていることを確認し、手順 1 ～ 5 を繰り返して証明書を再生成します。	（任意） 正しい使用期限が設定された証明書が作成されます。

この例は、CA の作成方法、および新規に作成された CA が署名するサーバ証明書の生成方法を示します。これらのコマンドは、OpenSSL を実行している Linux サーバで入力します。

```
# /usr/bin/openssl genrsa -out ca.key 2048
Generating RSA private key, 2048 bit long modulus
.............++++++
.....++++++
e is 65537 (0x10001)
# /usr/bin/openssl req -new -x509 -days 365 -key ca.key -out ca.crt
You are about to be asked to enter information that will be incorporated
```

```
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:California
Locality Name (eg, city) [Newbury]:San Jose
Organization Name (eg, company) [My Company Ltd]:Example Incorporated
Organizational Unit Name (eg, section) []:Unit A
Common Name (eg, your name or your server's hostname) []:example.com
Email Address []:admin@example.com
# echo "nsCertType = server" > openssl.conf
# /usr/bin/openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 01 -CAkey ca.key -out server.crt
-extfile openssl.conf
Signature ok
subject=/C=US/ST=California/L=San Jose/O=Example Inc./OU=Unit
A/CN=example.com/emailAddress=john@example.com
Getting CA Private Key
#
```

次の作業

新しい証明書を Cisco IMCにアップロードします。

Windows を使用した自己署名証明書の作成

はじめる前に

- 証明書を設定するには、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。
- Cisco IMC の時刻が現在の時刻に設定されていることを確認してください。

手順

ステップ 1 [IIS マネージャ（IIS Manager）] を開いて管理するレベルに移動します。

ステップ 2 [Features] 領域で、[サーバー証明書] をダブルクリックします。

ステップ 3 [操作] ペインで、[Create Self-Signed Certificate] をクリックします。

ステップ 4 [Create Self-Signed Certificate] ウィンドウで、[Specify a friendly name for the certificate] フィールドに証明書の名前を入力します。

ステップ 5 [OK] をクリックします。

ステップ 6 （任意） 生成された証明書に正しい使用期限が設定されていない場合は、Cisco IMC の時刻が現在の時刻に設定されていることを確認し、手順 1 ～ 5 を繰り返して証明書を再生成します。
正しい使用期限が設定された証明書が作成されます。

サーバ証明書のアップロード

サーバにアップロードする証明書を参照して選択するか、または署名付き証明書のすべての内容をコピーして [証明書コンテンツの貼り付け（Paste certificate content）] テキスト フィールドに貼り付け、それをアップロードできます。

はじめる前に

- 証明書をアップロードするには、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。
- アップロードする証明書ファイルは、ローカルにアクセスできるファイル システムに配置されている必要があります。
- 生成された証明書のタイプが [サーバ（Server）] であることを確認します。

（注） [証明書の管理（Cisco IMC Certificate Management）] メニューを使用して最初に CSR を生成してから、その CSR を使用してアップロードする証明書を取得する必要があります。この方法で取得されていない証明書はアップロードしないでください。

手順

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

ステップ 2 [管理者（Admin）] メニューの [証明書の管理（Certificate Management）] をクリックします。

ステップ 3 [アクション（Actions）] 領域で、[サーバ証明書のアップロード（Upload Server Certificate）] をクリックします。
[証明書のアップロード（Upload Certificate）] ダイアログボックスが表示されます。

ステップ 4 [証明書のアップロード（Upload Certificate）] ダイアログボックスで、次のプロパティを更新します。

[名前（Name）]	**説明**
[ファイル（File）] フィールド	アップロードする証明書ファイル。
[参照（Browse）] ボタン	適切な証明書ファイルに移動できるダイアログボックスが表示されます。

[名前（Name）]	説明
[証明書コンテンツの貼り付け（Paste Certificate content）] オプション ボタン	署名付き証明書のすべての内容をコピーして、[証明書コンテンツの貼り付け（Paste certificate content）] テキスト フィールドに貼り付けることができるダイアログボックスが開きます。 （注） アップロードする前に証明書が署名済みであることを確認します。
[証明書のアップロード（Upload Certificate）] ボタン	証明書をアップロードできます。

ステップ 5 [証明書のアップロード（Upload Certificate）] をクリックします。

キー管理相互運用性プロトコル

キー管理相互運用性プロトコル（KMIP）は、主要な管理サーバでキーまたは機密データを処理するためのメッセージ形式を定義する通信プロトコルです。KMIP はオープン スタンダードで、複数のベンダーによってサポートされています。キー管理には、複数の相互運用可能な実装が伴うため、KMIP クライアントは KMIP サーバと効率的に連動します。

自己暗号化ドライブ（SED）には、リアルタイムで着信データを暗号化し、発信データを復号化するハードウェアが含まれています。ドライブまたはメディア暗号化キーは、この機能を制御します。しかし、セキュリティを維持するために、ドライブはロックされている必要があります。セキュリティ キー ID とセキュリティ キー（キー暗号キー）を使用すると、この目的を達成できます。キー ID では、ドライブに一意の ID が提供されます。

異なるキーには異なる使用要件があります。現在、ローカル キーの管理および追跡の責任は主にユーザにあるため、人的ミスが生じる可能性があります。ユーザはさまざまなキーとそれらの機能を覚えている必要があり、それが困難な場合があります。KMIP は、この懸念領域に対処し、人的関与なしでキーを効率的に管理します。

セキュアなキー管理設定の表示

手順

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

ステップ 2 [管理者（Admin）] メニューの [セキュリティ管理（Security Management）] をクリックします。

ステップ 3 [セキュリティ管理（Security Management）] ペインの [セキュアなキー管理（Secure Key Management）] をクリックします。

ステップ 4 [作業（Work）] ペインで、次の情報を確認します。

名称	説明
[セキュアなキー管理の有効化（Enable Secure Key Management）] チェックボックス	オンにすると、セキュアなキー管理機能を有効にできます。

ステップ 5 [アクション（Actions）] 領域で、次の情報を確認します。

名称	説明
[ルート CA 証明書のダウンロード（Download Root CA Certificate）] リンク	ルート CA 証明書を Cisco IMC にダウンロードできます。
[ルート CA 証明書のエクスポート（Export Root CA Certificate）] リンク	ダウンロードしたルート CA 証明書をローカルファイルまたはリモートサーバにエクスポートできます。
[ルート CA 証明書の削除（Delete Root CA Certificate）] リンク	ルート CA 証明書を削除できます。
[クライアント証明書のダウンロード（Download Client Certificate）] リンク	クライアント証明書を Cisco IMC にダウンロードできます。
[クライアント証明書のエクスポート（Export Client Certificate）] リンク	ダウンロードしたクライアント証明書をローカルファイルまたはリモートサーバにエクスポートできます。
[クライアント証明書の削除（Delete Client Certificate）] リンク	クライアント証明書を削除できます。
[クライアント秘密キーのダウンロード（Download Client Private Key）] リンク	クライアント秘密キーを Cisco IMC にダウンロードできます。

名称	説明
[クライアント秘密キーのエクスポート（Export Client Private Key）] リンク	ダウンロードしたルート CA 証明書をローカルファイルまたはリモートサーバにエクスポートできます。
[クライアント秘密キーの削除（Delete Client Private Key）] リンク	ルート CA 証明書を削除できます。
[KMIP ログインの削除（Delete KMIP Login）] リンク	KMIP ログインの詳細を削除できます。

ステップ 6 [KMIP サーバ（KMIP Servers）] 領域で、次のフィールドを確認します。

名称	説明
[ID] フィールド	KMIP サーバ設定の ID。
[IPアドレス（IP Address）] フィールド	KMIP サーバの IP アドレス。
[ポート（Port）] フィールド	KMIP サーバへの通信ポート。
[タイムアウト（Timeout）] フィールド	Cisco IMC が KMIP サーバからの応答を待機する時間。
[削除（Delete）] ボタン	KMIP サーバ設定を削除します。
[テスト接続（Test Connection）] ボタン	KMIP接続が成功したかどうかをテストします。

ステップ 7 [KMIP ルート CA 証明書（KMIP Root CA Certificate）] 領域で、次のフィールドを確認します。

名称	説明
[サーバ ルート CA 証明書（Server Root CA Certificate）] フィールド	ルート CA 証明書の可用性を示します。
[ダウンロード ステータス（Download Status）] フィールド	このフィールドには、ルート CA 証明書のダウンロード ステータスが表示されます。
[ダウンロードの進行状況（Download Progress）] フィールド	このフィールドには、ルート CA 証明書のダウンロードの進行状況が表示されます。
[エクスポート ステータス（Export Status）] フィールド	このフィールドには、ルート CA 証明書のエクスポート ステータスが表示されます。

名称	説明
[エクスポートの進行状況（Export Progress）] フィールド	このフィールドには、ルート CA 証明書のエクスポートの進行状況が表示されます。

ステップ 8 [KMIP クライアント証明書（KMIP Client Certificate）] 領域で、次のフィールドを確認します。

名称	説明
[クライアント証明書（Client Certificate）] フィールド	クライアント証明書の可用性を示します。
[ダウンロード ステータス（Download Status）] フィールド	このフィールドには、クライアント証明書のダウンロード ステータスが表示されます。
[ダウンロードの進行状況（Download Progress）] フィールド	このフィールドには、クライアント証明書のダウンロードの進行状況が表示されます。
[エクスポート ステータス（Export Status）] フィールド	このフィールドには、クライアント証明書のエクスポート ステータスが表示されます。
[エクスポートの進行状況（Export Progress）] フィールド	このフィールドには、クライアント証明書のエクスポートの進行状況が表示されます。

ステップ 9 [KMIP ログインの詳細（KMIP Login Details）] 領域で、次のフィールドを確認します。

名称	説明
[KMIP ログインを使用（Use KMIP Login）] チェック ボックス	KMIP ログインの詳細を使用するかどうかを選択できます。
[KMIP サーバへのログイン名（Login name to KMIP Server）] フィールド	KMIP サーバのユーザ名。
[KMIP サーバへのパスワード（Password to KMIP Server）] フィールド	KMIP サーバのパスワード。
[パスワードの変更（Change Password）] チェックボックス	KMIP パスワードを変更できます。

名称	説明
[新しいパスワード（New Password）] フィールド	KMIP サーバに割り当てる新しいパスワードを入力できます。 （注） このオプションは、[パスワードの変更（Change Password）] チェックボックスを有効にしている場合にのみ表示されます。
[パスワードの確認（Confirm Password）] フィールド	このフィールドにもう一度新しいパスワードを入力します。 （注） このオプションは、[パスワードの変更（Change Password）] チェックボックスを有効にしている場合にのみ表示されます。

ステップ 10 [KMIP クライアント秘密キー（KMIP Client Private Key）] 領域で、次のフィールドを確認します。

名称	説明
[クライアント秘密キー（Client Private Key）] フィールド	クライアント秘密キーの可用性を示します。
[ダウンロード ステータス（Download Status）] フィールド	このフィールドには、クライアント秘密キーのダウンロード ステータスが表示されます。
[ダウンロードの進行状況（Download Progress）] フィールド	このフィールドには、クライアント秘密キーのダウンロードの進行状況が表示されます。
[エクスポート ステータス（Export Status）] フィールド	このフィールドには、クライアント秘密キーのエクスポート ステータスが表示されます。
[エクスポートの進行状況（Export Progress）] フィールド	このフィールドには、クライアント秘密キーのエクスポートの進行状況が表示されます。

KMIP 設定のクライアント秘密キーおよびクライアント証明書の作成

パブリック認証局（CA）を使用してサーバ証明書の生成と署名を行う代わりに、独自の CA を運用して独自の証明書に署名することができます。このセクションでは、Linux で実行されている

OpenSSL 証明書サーバを使用して CA を作成するコマンドおよびサーバ証明書を生成するコマンドについて説明します。OpenSSL の詳細については、http://www.openssl.orgを参照してください。

（注） これらのコマンドは、Cisco IMC ではなく、OpenSSL パッケージを使用している Linux サーバで入力します。

はじめる前に

- 組織内のサーバで、証明書サーバのソフトウェア パッケージを取得してインストールします。
- Cisco IMC の時刻が現在の時刻に設定されていることを確認してください。

手順

	コマンドまたはアクション	目的
ステップ 1	**openssl genrsa -out** *Client_Privatekeyfilename keysize* 例： `# openssl genrsa -out client_private.pem 2048`	このコマンドは、クライアント証明書の生成に使用されるクライアント秘密キーを生成します。 指定されたファイル名には、指定されたサイズの RSA キーが含まれています。
ステップ 2	**openssl req -new -x509 -days** *numdays***-key** *Client_Privatekeyfilename***-out** *Client_certfilename* 例： `# openssl req -new -x509 -key client_private.pem -out client.pem -days 365`	このコマンドは、前の手順で入手したクライアント秘密キーを使用して、新しい自己署名クライアント証明書を生成します。証明書は指定された期間有効になります。このコマンドは、ユーザに証明書の追加情報を求めるプロンプトを表示します。 新しい自己署名クライアント証明書が作成されます。
ステップ 3	KMIP サーバから KMIP ルート CA 証明書を取得します。	ルート CA 証明書の取得については、KMIP のベンダー マニュアルを参照してください。

次の作業

新しい証明書を Cisco IMCにアップロードします。

クライアント証明書のダウンロード

手順

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

ステップ 2 [管理者（Admin）] メニューの [セキュリティ管理（Security Management）] をクリックします。

ステップ 3 [セキュリティ管理（Security Management）] ペインの [セキュアなキー管理（Secure Key Management）] をクリックします。

ステップ 4 [セキュアなキー管理（Secure Key Management）] タブの [アクション（Actions）] 領域で、[クライアント証明書のダウンロード（Download Client Certificate）] をクリックします。

ステップ 5 [クライアント証明書のダウンロード（Download Client Certificate）] ダイアログボックスで、次のフィールドに値を入力します。

[名前（Name）]	説明
[リモート ロケーションからダウンロード（Download From Remote Location）] オプション ボタン	このオプションを選択することで、証明書をリモートの場所から選択してダウンロードできます。次の詳細を入力します。 • ◦ TFTP サーバ（TFTP Server） ◦ FTP サーバ（FTP Server） ◦ SFTP サーバ（SFTP Server） ◦ SCP サーバ ◦ HTTP サーバ（HTTP Server） （注） このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「サーバ（*RSA*）キー 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?*）」というメッセージとともにポップアップ ウィンドウが表示されます。サーバ フィンガープリントの信頼性に応じて、[はい（Yes）] または [いいえ（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に基づいており、接続先のホストを識別または確認できます。 • [サーバ IP/ホスト名（Server IP/Hostname）] フィールド：クライアント証明書ファイルを保管するサーバの IP アドレスまたはホスト名。[証明書のダウンロード元（Download Certificate from）] ドロップダウン リストの設定によって、このフィールドの名前は異なる場合があります。 • [パスおよびファイル名（Path and Filename）] フィールド：リモート サーバにファイルをダウンロードする際に Cisco IMC で使用するパスおよびファイル名。 • [ユーザ名（Username）] フィールド：システムがリモート サーバにログインする際に使用するユーザ名。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。 • [パスワード（Password）] フィールド：リモート サーバのユーザ名に対応するパスワード。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。

[名前（Name）]	説明
[ブラウザ クライアント経由でダウンロード（Download Through Browser Client）] オプション ボタン	このオプションを選択することで、Cisco IMC GUI を実行しているコンピュータのローカル ドライブに保管されている証明書に移動できます。 このオプションを選択すると、Cisco IMC GUI に [参照（Browse）] ボタンが表示されます。このボタンを使用して、インポートするファイルに移動できます。
[コンテンツの貼り付け（Paste Content）] オプション ボタン	このオプションを選択することで、署名付き証明書の内容全体をコピーして [証明書コンテンツの貼り付け（Paste Certificate Content）] テキスト フィールドに貼り付けることができます。 （注） アップロードする前に証明書が署名済みであることを確認します。

クライアント証明書のエクスポート

手順

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

ステップ 2 [管理者（Admin）] メニューの [セキュリティ管理（Security Management）] をクリックします。

ステップ 3 [セキュリティ管理（Security Management）] ペインの [セキュアなキー管理（Secure Key Management）] をクリックします。

ステップ 4 [セキュアなキー管理（Secure Key Management）] タブの [アクション（Actions）] 領域で、[クライアント証明書のエクスポート（Export Client Certificate）] をクリックします。

ステップ 5 [クライアント証明書のエクスポート（Export Client Certificate）] ダイアログボックスで、次のフィールドに値を入力します。

[名前（Name）]	説明
[リモートロケーションにエクスポート（Export to Remote Location）[	

[名前（Name）]	説明
	このオプションを選択することで、証明書をリモートの場所から選択してエクスポートできます。次の詳細を入力します。 • ◦ TFTP サーバ（TFTP Server） ◦ FTP サーバ（FTP Server） ◦ SFTP サーバ（SFTP Server） ◦ SCP サーバ ◦ HTTP サーバ（HTTP Server） （注） このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「サーバ（*RSA*）キー 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?*）」というメッセージとともにポップアップ ウィンドウが表示されます。サーバ フィンガープリントの信頼性に応じて、[はい（Yes）] または [いいえ（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に基づいており、接続先のホストを識別または確認できます。 • [サーバ IP/ホスト名（Server IP/Hostname）] フィールド：証明書ファイルをエクスポートするサーバの IP アドレスまたはホスト名。[証明書のダウンロード元（Download Certificate from）] ドロップダウン リストの設定によって、このフィールドの名前は異なる場合があります。 • [パスおよびファイル名（Path and Filename）] フィールド：リモート サーバから証明書をダウンロードする際に Cisco IMC が使用するパスおよびファイル名。

[名前（Name）]	説明
	• [ユーザ名（Username）] フィールド：システムがリモート サーバにログインする際に使用するユーザ名。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。 • [パスワード（Password）] フィールド：リモート サーバのユーザ名に対応するパスワード。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。
ローカル ファイルにエクスポート（Export to Local File）	このオプションを選択することで、コンピュータのローカル ドライブに保管されている証明書を選択してエクスポートできます。

クライアント証明書の削除

手順

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

ステップ 2 [管理者（Admin）] メニューの [セキュリティ管理（Security Management）] をクリックします。

ステップ 3 [セキュリティ管理（Security Management）] ペインの [セキュアなキー管理（Secure Key Management）] をクリックします。

ステップ 4 [セキュアなキー管理（Secure Key Management）] タブの [アクション（Actions）] 領域で、[クライアント証明書の削除（Delete Client Certificate）] をクリックします。

ステップ 5 プロンプトで、[OK] をクリックしてクライアント証明書を削除するか、または [キャンセル（Cancel）] をクリックして操作をキャンセルします。

ルート CA 証明書のダウンロード

手順

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

ステップ 2 [管理者（Admin）] メニューの [セキュリティ管理（Security Management）] をクリックします。

ステップ 3 [セキュリティ管理（Security Management）] ペインの [セキュアなキー管理（Secure Key Management）] をクリックします。

ステップ 4 [セキュアなキー管理（Secure Key Management）] タブの [アクション（Actions）] 領域で、[ルート CA 証明書のダウンロード（Download Root CA Certificate）] をクリックします。

ステップ 5 [ルート CA 証明書のダウンロード（Download Root CA Certificate）] ダイアログボックスで、次のフィールドに値を入力します。

[名前（Name）]	説明
[リモート ロケーションからダウンロード（Download From Remote Location）] オプション ボタン	このオプションを選択することで、証明書をリモートの場所から選択してダウンロードできます。次の詳細を入力します。 • ◦ TFTP サーバ（TFTP Server） ◦ FTP サーバ（FTP Server） ◦ SFTP サーバ（SFTP Server） ◦ SCP サーバ ◦ HTTP サーバ（HTTP Server） （注） このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「サーバ（*RSA*）キー 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?*）」というメッセージとともにポップアップ ウィンドウが表示されます。サーバ フィンガープリントの信頼性に応じて、[はい（Yes）] または [いいえ（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に基づいており、接続先のホストを識別または確認できます。 • [サーバ IP/ホスト名（Server IP/Hostname）] フィールド：ルート CA 証明書ファイルを保管するサーバの IP アドレスまたはホスト名。[証明書のダウンロード元（Download Certificate from）] ドロップダウン リストの設定によって、このフィールドの名前は異なる場合があります。 • [パスおよびファイル名（Path and Filename）] フィールド：リモート サーバにファイルをダウンロードする際に Cisco IMC で使用するパスおよびファイル名。 • [ユーザ名（Username）] フィールド：システムがリモート サーバにログインする際に使用するユーザ名。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。 • [パスワード（Password）] フィールド：リモート サーバのユーザ名に対応するパスワード。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。

[名前（Name）]	説明
[ブラウザ クライアント経由でダウンロード（Download Through Browser Client）] オプション ボタン	このオプションを選択することで、Cisco IMC GUI を実行しているコンピュータのローカル ドライブに保管されている証明書に移動できます。 このオプションを選択すると、Cisco IMC GUI に [参照（Browse）] ボタンが表示されます。このボタンを使用して、インポートするファイルに移動できます。
[コンテンツの貼り付け（Paste Content）] オプション ボタン	このオプションを選択することで、署名付き証明書の内容全体をコピーして [証明書コンテンツの貼り付け（Paste Certificate Content）] テキスト フィールドに貼り付けることができます。 （注） アップロードする前に証明書が署名済みであることを確認します。

ルート CA 証明書のエクスポート

手順

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

ステップ 2 [管理者（Admin）] メニューの [セキュリティ管理（Security Management）] をクリックします。

ステップ 3 [セキュリティ管理（Security Management）] ペインの [セキュアなキー管理（Secure Key Management）] をクリックします。

ステップ 4 [セキュアなキー管理（Secure Key Management）] タブの [アクション（Actions）] 領域で、[ルート CA 証明書のエクスポート（Export Root CA Certificate）] をクリックします。

ステップ 5 [ルート CA 証明書のエクスポート（Export Root CA Certificate）] ダイアログボックスで、次のフィールドに値を入力します。

[名前（Name）]	説明
[リモートロケーションにエクスポート（Export to Remote Location）[	

[名前（Name）]	説明
	このオプションを選択することで、証明書をリモートの場所から選択してエクスポートできます。次の詳細を入力します。 • ◦ TFTP サーバ（TFTP Server） ◦ FTP サーバ（FTP Server） ◦ SFTP サーバ（SFTP Server） ◦ SCP サーバ ◦ HTTP サーバ（HTTP Server） （注） このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「サーバ（*RSA*）キー 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?*）」というメッセージとともにポップアップ ウィンドウが表示されます。サーバ フィンガープリントの信頼性に応じて、[はい（Yes）] または [いいえ（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に基づいており、接続先のホストを識別または確認できます。 • [サーバ IP/ホスト名（Server IP/Hostname）] フィールド：証明書ファイルをエクスポートするサーバの IP アドレスまたはホスト名。[証明書のダウンロード元（Download Certificate from）] ドロップダウン リストの設定によって、このフィールドの名前は異なる場合があります。 • [パスおよびファイル名（Path and Filename）] フィールド：リモート サーバから証明書をダウンロードする際に Cisco IMC が使用するパスおよびファイル名。

[名前（Name）]	説明
	• [ユーザ名（Username）] フィールド：システムがリモート サーバにログインする際に使用するユーザ名。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。 • [パスワード（Password）] フィールド：リモート サーバのユーザ名に対応するパスワード。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。
ローカル ファイルにエクスポート（Export to Local File）	このオプションを選択することで、コンピュータのローカル ドライブに保管されている証明書を選択してエクスポートできます。

ルート CA 証明書の削除

手順

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

ステップ 2 [管理者（Admin）] メニューの [セキュリティ管理（Security Management）] をクリックします。

ステップ 3 [セキュリティ管理（Security Management）] ペインの [セキュアなキー管理（Secure Key Management）] をクリックします。

ステップ 4 [セキュアなキー管理（Secure Key Management）] タブの [アクション（Actions）] 領域で、[ルート CA 証明書の削除（Delete Root CA Certificate）] をクリックします。

ステップ 5 プロンプトで、[OK] をクリックしてルート CA 証明書を削除するか、または [キャンセル（Cancel）] をクリックして操作をキャンセルします。

クライアント秘密キーのダウンロード

手順

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

ステップ 2 [管理者（Admin）] メニューの [セキュリティ管理（Security Management）] をクリックします。

ステップ 3 [セキュリティ管理（Security Management）] ペインの [セキュアなキー管理（Secure Key Management）] をクリックします。

ステップ 4 [セキュアなキー管理（Secure Key Management）] タブの [アクション（Actions）] 領域で、[クライアント秘密キーのダウンロード（Download Client Private Key）] をクリックします。

ステップ 5 [クライアント秘密キーのダウンロード（Download Client Private Key）] ダイアログボックスで、次のフィールドに値を入力します。

[名前（Name）]	説明
[リモート ロケーションからダウンロード（Download From Remote Location）] オプション ボタン	このオプションを選択することで、秘密キーをリモートの場所から選択してダウンロードできます。次の詳細を入力します。 • ◦ TFTP サーバ（TFTP Server） ◦ FTP サーバ（FTP Server） ◦ SFTP サーバ（SFTP Server） ◦ SCP サーバ ◦ HTTP サーバ（HTTP Server） （注） このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「サーバ（*RSA*）キー 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?*）」というメッセージとともにポップアップ ウィンドウが表示されます。サーバ フィンガープリントの信頼性に応じて、[はい（Yes）] または [いいえ（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に基づいており、接続先のホストを識別または確認できます。 • [サーバ IP/ホスト名（Server IP/Hostname）] フィールド：クライアント秘密キーを保管するサーバの IP アドレスまたはホスト名。[証明書のダウンロード元（Download Certificate From）] ドロップダウン リストの設定によって、このフィールドの名前は異なる場合があります。 • [パスおよびファイル名（Path and Filename）] フィールド：リモート サーバにファイルをダウンロードする際に Cisco IMC で使用するパスおよびファイル名。 • [ユーザ名（Username）] フィールド：システムがリモート サーバにログインする際に使用するユーザ名。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。 • [パスワード（Password）] フィールド：リモート サーバのユーザ名に対応するパスワード。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。

[名前（Name）]	説明
[ブラウザ クライアント経由でダウンロード（Download Through Browser Client）] オプション ボタン	このオプションを選択することで、Cisco IMC GUI を実行しているコンピュータのローカル ドライブに保管されている秘密キーに移動できます。 このオプションを選択すると、Cisco IMC GUI に [参照（Browse）] ボタンが表示されます。このボタンを使用して、インポートするファイルに移動できます。
[コンテンツの貼り付け（Paste Content）] オプション ボタン	このオプションを選択することで、署名付き秘密キーの内容全体をコピーして [秘密キー コンテンツの貼り付け（Paste Private Key Content）] テキスト フィールドに貼り付けることができます。

次の作業

クライアント秘密キーのエクスポート

手順

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

ステップ 2 [管理者（Admin）] メニューの [セキュリティ管理（Security Management）] をクリックします。

ステップ 3 [セキュリティ管理（Security Management）] ペインの [セキュアなキー管理（Secure Key Management）] をクリックします。

ステップ 4 [セキュアなキー管理（Secure Key Management）] タブの [アクション（Actions）] 領域で、[クライアント秘密キーのエクスポート（Export Client Private Key）] をクリックします。

ステップ 5 [クライアント秘密キーのエクスポート（Export Client Private Key）] ダイアログボックスで、次のフィールドに値を入力します。

[名前（Name）]	説明
[リモートロケーションにエクスポート（Export to Remote Location）[	

[名前（Name）]	説明
	このオプションを選択することで、証明書をリモートの場所から選択してエクスポートできます。次の詳細を入力します。 • ◦ TFTP サーバ（TFTP Server） ◦ FTP サーバ（FTP Server） ◦ SFTP サーバ（SFTP Server） ◦ SCP サーバ ◦ HTTP サーバ（HTTP Server） （注） このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「サーバ（*RSA*）キー 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?*）」というメッセージとともにポップアップ ウィンドウが表示されます。サーバ フィンガープリントの信頼性に応じて、[はい（Yes）] または [いいえ（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に基づいており、接続先のホストを識別または確認できます。 • [サーバ IP/ホスト名（Server IP/Hostname）] フィールド：証明書ファイルをエクスポートするサーバの IP アドレスまたはホスト名。[証明書のダウンロード元（Download Certificate from）] ドロップダウン リストの設定によって、このフィールドの名前は異なる場合があります。 • [パスおよびファイル名（Path and Filename）] フィールド：リモート サーバから証明書をダウンロードする際に Cisco IMC が使用するパスおよびファイル名。

[名前（Name）]	説明
	• [ユーザ名（Username）] フィールド：システムがリモート サーバにログインする際に使用するユーザ名。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。 • [パスワード（Password）] フィールド：リモート サーバのユーザ名に対応するパスワード。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。
ローカル ファイルにエクスポート（Export to Local File）	このオプションを選択することで、コンピュータのローカル ドライブに保管されている証明書を選択してエクスポートできます。

クライアント秘密キーの削除

手順

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

ステップ 2 [管理者（Admin）] メニューの [セキュリティ管理（Security Management）] をクリックします。

ステップ 3 [セキュリティ管理（Security Management）] ペインの [セキュアなキー管理（Secure Key Management）] をクリックします。

ステップ 4 [セキュアなキー管理（Secure Key Management）] ペインの [アクション（Actions）] 領域で、[クライアント秘密キーの削除（Delete Client Private Key）] をクリックします。

ステップ 5 プロンプトで、[OK] をクリックしてクライアント秘密キーを削除するか、または [キャンセル（Cancel）] をクリックして操作をキャンセルします。

KMIP サーバ接続のテスト

手順

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

ステップ 2 [管理者（Admin）] メニューの [セキュリティ管理（Security Management）] をクリックします。

ステップ 3 [セキュリティ管理（Security Management）] ペインの [セキュアなキー管理（Secure Key Management）] をクリックします。

ステップ 4 [セキュアなキー管理（Secure Key Management）] タブの [KMIP サーバ（KMIP Servers）] 領域で、チェックボックスをオンにすることで行を選択し、[テスト接続（Test Connection）] をクリックします。

ステップ 5 接続に成功すると、成功メッセージが表示されます。

KMIP サーバのデフォルト設定への復元

手順

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

ステップ 2 [管理者（Admin）] メニューの [セキュリティ管理（Security Management）] をクリックします。

ステップ 3 [セキュリティ管理（Security Management）] ペインの [セキュアなキー管理（Secure Key Management）] をクリックします。

ステップ 4 [セキュアなキー管理（Secure Key Management）] タブの [KMIP サーバ（KMIP Servers）] 領域で、チェックボックスをオンにすることで行を選択し、[削除（Delete）] をクリックします。

ステップ 5 プロンプトで [OK] をクリックします。
これで、KMIP サーバがデフォルト設定に復元されます。

KMIP ログイン詳細の削除

手順

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

ステップ 2 [管理者（Admin）] メニューの [セキュリティ管理（Security Management）] をクリックします。

ステップ 3 [セキュリティ管理（Security Management）] ペインの [セキュアなキー管理（Secure Key Management）] をクリックします。

ステップ 4 [セキュアなキー管理（Secure Key Management）] ペインの [アクション（Actions）] 領域で、[KMIP ログインの削除（Delete KMIP Login）] をクリックします。

ステップ 5 プロンプトで、[OK] をクリックして KMIP ログインの詳細を削除するか、または [キャンセル（Cancel）] をクリックして操作をキャンセルします。

第 15 章

ファームウェアの管理

この章の内容は、次のとおりです。

Cisco IMC ファームウェア

Web UI の単一ページから次のファームウェア コンポーネントを管理できます。

- アダプタ ファームウェア：アクティブなイメージとバックアップ イメージで構成されている主要なオペレーティング ファームウェアで、次のような異なるインターフェイスからインストールできます。
  - ホスト アップグレード ユーティリティ（HUU）
  - Web UI：ローカルおよびリモートのプロトコル
  - PMCLI：リモート プロトコル
  - XML API：リモート プロトコル

  ファームウェア イメージをローカル ファイル システムまたは TFTP サーバからアップロードできます。
- ブートローダ ファームウェア：ブートローダ ファームウェアは、Cisco IMC からインストールできません。このファームウェアは、Host Upgrade Utility を使用してインストールできます。

次の個々のコンポーネントのファームウェアを更新できます。

- BMC

- BIOS
- CMC
- SAS エクスパンダ
- アダプタ

ハード ディスク ドライブ（HDD）のファームウェアは、上述のアダプタ ファームウェアと同じインターフェイスからインストールすることもできます。

ファームウェア コンポーネントの表示

手順

ステップ 1 [管理者（Admin）] メニューの [ファームウェア管理（Firmware Management）] をクリックします。

ステップ 2 [全般（General）] タブの [ファームウェア管理（Firmware Management）] 領域で、次の情報を確認します。

[名前（Name）]	**説明**
[更新（Update）] ボタン	ダイアログボックスが開き、ローカルマシンまたはリモートサーバで利用可能なファームウェアイメージファイルをインストールできます。
[アクティブ化（Activate）] ボタン	ダイアログボックスが開き、サーバでアクティブにする使用可能なファームウェアバージョンを選択できます。 **重要** ファームウェアまたは BIOS のアップデートが進行中の場合は、それらのタスクが完了するまで新しいファームウェアをアクティブにしないでください。
[コンポーネント（Component）] 列	ファームウェアを更新できる使用可能なコンポーネントのリスト。
[稼働バージョン（Running Version）] カラム	現在有効なコンポーネントのファームウェアバージョン。

[名前（Name）]	説明
[バックアップバージョン（Backup Version）] カラム	サーバにインストールされている別のファームウェア バージョン（存在する場合）。バックアップ バージョンは現在動作していません。これをアクティブにするには、[アクティブ化（Activate）] をクリックします。 （注） 新しいファームウェアをインストールすると、既存のバックアップ バージョンはすべて削除され、新しいファームウェアがバックアップ バージョンになります。サーバで新しいバージョンを実行するには、新しいファームウェアを手動でアクティブにする必要があります。
[ブートローダーのバージョン（Bootloader Version）] カラム	コンポーネントのブートローダ ソフトウェアに関連付けられているブートローダ バージョン。
[ステータス（Status）] カラム	このサーバのファームウェアのアクティブ化のステータス。
[進行状況 %（Progress in %）] カラム	操作の進行状況のパーセンテージ。

ファームウェアの更新

[ファームウェア管理（Firmware Management）] 領域から選択したコンポーネントに応じて、ローカル ディスクまたはリモート サーバからファームウェア パッケージをインストールできます。インストールを確認した後、BMC によってコンポーネントのバックアップ メモリ スロット内のファームウェア バージョンが選択したバージョンに置き換えられます。

手順

ステップ 1 [管理者（Admin）] メニューの [ファームウェア管理（Firmware Management）] をクリックします。

ステップ 2 [ファームウェア管理（Firmware Management）] 領域で、[コンポーネント（Component）] カラムからコンポーネントを選択し、[更新（Update）] をクリックします。
[ファームウェアの更新（Update Firmware）] ダイアログボックスが表示されます。

ステップ 3 ダイアログボックスで次の情報を確認します。

[名前（Name）]	説明
[ブラウザ クライアントによるファームウェアのインストール（Install Firmware through Browser Client）] オプション ボタン	ファームウェア パッケージがローカル マシンに存在する場合は、このオプション ボタンをクリックします。
[リモート サーバによるファームウェアのインストール（Install Firmware through Remote Server）] オプション ボタン	ファームウェア パッケージがリモート サーバに存在する場合は、このオプション ボタンをクリックします。

ステップ 4 ブラウザ クライアントを介してファームウェアをインストールするには、[参照（Browse）] をクリックし、インストールするファームウェア ファイルに移動します。

ステップ 5 ファイルを選択してから、[ファームウェアのインストール（Install Firmware）] をクリックします。

ステップ 6 リモート サーバを使用してファームウェアを更新するには、[ファームウェアのインストール元（Install Firmware from）] ドロップダウン リストからリモート サーバのタイプを選択します。次のいずれかを選択できます。

- TFTP
- FTP
- SFTP
- SCP
- HTTP

ステップ 7 選択するリモート サーバのタイプに応じて、サーバの [IP/ホスト名（IP/Hostname）] フィールドと [イメージ パスとファイル名（Image Path and Filename）] フィールドに詳細を入力します。ファームウェアをインストールすると、新しいイメージが非アクティブなイメージと置き換わります。イメージのインストール後、イメージをアクティブ化ができます。

重要 サーバのタイプが FTP、SFTP、または SCP の場合は、ユーザ クレデンシャルを入力する必要があります。

ステップ 8 [ファームウェアのインストール（Install Firmware）] をクリックして、ダウンロードとインストールを開始します。

ファームウェアのアクティブ化

手順

ステップ 1 [管理者（Admin）] メニューの [ファームウェア管理（Firmware Management）] をクリックします。

ステップ 2 [ファームウェア管理（Firmware Management）] 領域で、[コンポーネント（Component）] カラムからコンポーネントを選択し、[アクティブ化（Activate）] をクリックします。
[ファームウェアの有効化（Activate Firmware）] ダイアログボックスが表示されます。

ステップ 3 [ファームウェアのアクティブ化（Activate Firmware）] ダイアログボックスで、アクティブにするファームウェアイメージ（オプションボタン）を選択します。このイメージが稼動バージョンになります。

ステップ 4 [ファームウェアの有効化（Activate Firmware）] をクリックします。
選択したファームウェア イメージに応じて、アクティブ化のプロセスが開始されます。

重要 アクティベーションの進行中には、次のことは行わないでください。

- サーバのリセット、電源オフ、またはシャットダウン。
- BMC のリブートまたはリセット
- 他のファームウェアのアクティブ化。
- テクニカル サポートまたは設定データのエクスポート。

第 16 章

障害およびログの表示

この章の内容は、次のとおりです。

障害サマリー

障害サマリーの表示

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 [障害およびログ（Faults and Logs）] をクリックします。

ステップ 3 [障害サマリー（Faults Summary）] タブで、次の情報を確認します。

表 *8* : *[アクション（Actions）]* 領域

[名前（Name）]	説明
[合計（Total）]	[障害エントリ（Fault Entries）] テーブルの合計行数を表示します。
[列（Column）] ドロップダウン リスト	表示する列を選択できます。

[名前（Name）]	説明
[表示（Show）] ドロップダウン リスト	フィルタを使用して障害のエントリを表示する方法をカスタマイズします。これらの内容は次のとおりです。 • [クイック フィルタ（Quick Filter）]：デフォルト ビュー。 • [高度なフィルタ（Advanced Filter）]：1 つ以上の条件に基づき障害エントリを表示するフィルタ オプション。一致するルールを使用して、すべてのルールまたは [フィルタ（Filter）] フィールドで指定したルールの任意の組み合わせに一致するエントリを表示できます。 設定したフィルタ条件に一致するエントリを表示するには、[移動（Go）] をクリックします。 設定したフィルタ条件を保存するには、[保存（Save）] アイコンをクリックします。これはユーザ定義のフィルタになり、後で使用できます。 （注） ユーザ定義のフィルタは、[プリセット フィルタの管理（Manage Preset Filters）] ダイアログボックスに表示されます。 • [すべて（All）]：すべてのエントリを表示します。 • [プリセット フィルタの管理（Manage Preset Filters）]：ユーザ定義のフィルタを表示します。このダイアログボックスからユーザ定義のフィルタを編集または削除できます。 • [事前定義フィルタのリスト（List of pre-defined filters）]：システム定義のフィルタを表示します。 （注） [フィルタ（Filter）] アイコンを使用して、フィルタ フィールドを非表示または非表示解除できます。

表 *9*：*[*障害エントリ（***Fault Entries***）*]* 領域

[名前（**Name**）]	説明
時刻（Time）	障害が発生した時刻。
重大度（Severity）	次のいずれかになります。 • [クリア済み（Cleared）]：ある障害または状態が解消されました。 • クリティカル（Critical） • 情報（Info） • [メジャー（Major）] • [マイナー（Minor）] • 警告
コード（Code）	障害に割り当てられた固有識別情報。
[DN]	識別名（DN）は、サーバ上でのデバイスのエンドポイントおよびそのインスタンスの階層表現です。
考えられる原因	障害の原因となったイベントに関連付けられた固有識別情報。
説明	障害についての詳細情報。 提案される解決策も含まれます。

障害履歴

障害履歴の表示

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 [障害およびログ（Faults and Logs）] をクリックします。

ステップ 3 [障害履歴（Faults History）] タブで、次の情報を確認します。

表 *10*：*[アクション（Actions）]* 領域

[名前（Name）]	**説明**
[合計（Total）]	[障害履歴（Fault History）] テーブルの合計行数を表示します。
[列（Column）] ドロップダウン リスト	表示する列を選択できます。

[名前（Name）]	説明
[表示（Show）] ドロップダウン リスト	フィルタを使用して障害履歴エントリを表示する方法をカスタマイズします。これらの内容は次のとおりです。 • [クイック フィルタ（Quick Filter）]：デフォルト ビュー。 • [高度なフィルタ（Advanced Filter）]：1 つ以上の条件に基づきエントリを表示するフィルタ オプション。一致するルールを使用して、すべてのルールまたは [フィルタ（Filter）] フィールドで指定したルールの任意の組み合わせに一致するエントリを表示できます。 設定したフィルタ条件に一致するエントリを表示するには、[移動（Go）] をクリックします。 設定したフィルタ条件を保存するには、[保存（Save）] アイコンをクリックします。これはユーザ定義のフィルタになり、後で使用できます。 （注） ユーザ定義のフィルタは、[プリセット フィルタの管理（Manage Preset Filters）] ダイアログボックスに表示されます。 • [すべて（All）]：すべてのエントリを表示します。 • [プリセット フィルタの管理（Manage Preset Filters）]：ユーザ定義のフィルタを表示します。このダイアログボックスからユーザ定義のフィルタを編集または削除できます。 • [事前定義フィルタのリスト（List of pre-defined filters）]：システム定義のフィルタを表示します。 （注） [フィルタ（Filter）] アイコンを使用して、フィルタ フィールドを非表示または非表示解除できます。

表 *11*：*[*障害履歴（*Faults History*）*]* 領域

[名前（**Name**）]	説明
時刻（Time）	障害が発生した時刻。
重大度（Severity）	次のいずれかになります。 • 緊急（Emergency） • アラート（Alert） • クリティカル（Critical） • エラー（Error） • 警告 • 通知（Notice） • 情報（Informational） • デバッグ（Debug）
ソース（Source）	イベントをログに記録したソフトウェア モジュール。
考えられる原因	障害の原因となったイベントに関連付けられた固有識別情報。
説明	障害についての詳細情報。 提案される解決策も含まれます。

次の作業

Cisco IMC ログ

Cisco IMC ログの表示

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 [障害およびログ（Faults and Logs）] をクリックします。

ステップ 3 [Cisco IMC ログ（Cisco IMC Log）] タブで、次の情報を確認します。

表 *12* : *[アクション（**Actions**）]* 領域

[名前（Name）]	説明
[ログの消去（Clear Log）] ボタン	すべてのログ ファイルを消去します。 （注） このオプションは、ユーザ ID が [admin] または [user] ユーザ ロールに割り当てられている場合にのみ使用できます。
[合計（Total）]	[Cisco IMC ログ（Cisco IMC Log）] テーブルの合計行数を表示します。
[列（Column）] ドロップダウン リスト	表示する列を選択できます。

[名前（Name）]	説明
[表示（Show）] ドロップダウン リスト	フィルタを使用して Cisco IMC ログ エントリを表示する方法をカスタマイズします。これらの内容は次のとおりです。 • [クイック フィルタ（Quick Filter）]：デフォルト ビュー。 • [高度なフィルタ（Advanced Filter）]：1 つ以上の条件に基づきログ エントリを表示するフィルタ オプション。一致するルールを使用して、すべてのルールまたは[フィルタ（Filter）] フィールドで指定したルールの任意の組み合わせに一致するエントリを表示できます。 設定したフィルタ条件に一致するエントリを表示するには、[移動（Go）] をクリックします。 設定したフィルタ条件を保存するには、[保存（Save）] アイコンをクリックします。これはユーザ定義のフィルタになり、後で使用できます。 （注） ユーザ定義のフィルタは、[プリセット フィルタの管理（Manage Preset Filters）] ダイアログボックスに表示されます。 • [すべて（All）]：すべてのエントリを表示します。 • [プリセット フィルタの管理（Manage Preset Filters）]：ユーザ定義のフィルタを表示します。このダイアログボックスからユーザ定義のフィルタを編集または削除できます。 • [事前定義フィルタのリスト（List of pre-defined filters）]：システム定義のフィルタを表示します。 （注） [フィルタ（Filter）] アイコンを使用して、フィルタ フィールドを非表示または非表示解除できます。

表 *13*：*[Cisco IMC* ログ（*Cisco IMC Log*）*]* テーブル

[名前（Name）]	説明
[時刻（Time）] カラム	イベントが発生した日時。
[重大度（Severity）] カラム	イベントの重大度。次のいずれかになります。 • 緊急（Emergency） • アラート（Alert） • クリティカル（Critical） • エラー（Error） • 警告 • 通知（Notice） • 情報（Informational） • デバッグ（Debug）
[ソース（Source）] カラム	イベントをログに記録したソフトウェア モジュール。
[説明（Description）] カラム	イベントの説明。

システム イベント ログ

システム イベント ログの表示

[システムイベントログ（System Event Log）] タブには、シスコ システム イベント ログ（Cisco SEL）の内部に保存される総容量である 131068 エントリに対して、最新の 3008 システム イベントのみが表示されます。Cisco SEL の最大容量（131068 レコード）に達すると、最も古いエントリが最新のエントリで上書きされます。

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 [障害およびログ（Faults and Logs）] をクリックします。

ステップ 3 [システム イベント ログ（System Event Log）] タブで、次の情報を確認します。

表 *14* : *[アクション（Actions）]* 領域

名称	説明
SEL フルネス インジケータ	[システムイベントログ（System Event Log）] タブの使用済み領域にパーセントで表示されます。この割合は 3008 エントリを基準として計算されます（[システムイベントログ（System Event Log）] タブには、常に最新の 3008 システムイベントのみが表示されます）。たとえば、[システムイベントログ（System Event Log）] タブに 1504 エントリがある場合、50 パーセントとして表示されます。 最初に 3008 エントリのセットに達した後は、SEL がクリアされるまで、状態は常に 100% として表示されます。
[ログの消去（Clear Log）] ボタン	ログ ファイルからすべてのイベントをクリアします。 （注） このオプションは、ユーザ ID が [admin] または [user] ユーザ ロールに割り当てられている場合にのみ使用できます。
[シャーシ（Chassis）] ドロップダウン リスト	ログを表示するシャーシまたはサーバを選択します。
[合計（Total）]	[システム イベント ログ（System Event Log）] テーブルの合計行数を表示します。
[列（Column）] ドロップダウン リスト	表示する列を選択できます。

名称	説明
[表示（Show）] ドロップダウン リスト	フィルタを使用してイベントを表示する方法をカスタマイズします。これらの内容は次のとおりです。 • [クイック フィルタ（Quick Filter）]：デフォルト ビュー。 • [高度なフィルタ（Advanced Filter）]：1 つ以上の条件に基づきイベントを表示するフィルタ オプション。一致するルールを使用して、すべてのルールまたは [フィルタ（Filter）] フィールドで指定したルールの任意の組み合わせに一致するエントリを表示できます。 設定したフィルタ条件に一致するエントリを表示するには、[移動（Go）] をクリックします。 設定したフィルタ条件を保存するには、[保存（Save）] アイコンをクリックします。これはユーザ定義のフィルタになり、後で使用できます。 （注） ユーザ定義のフィルタは、[プリセット フィルタの管理（Manage Preset Filters）] ダイアログボックスに表示されます。 • [すべて（All）]：すべてのエントリを表示します。 • [プリセット フィルタの管理（Manage Preset Filters）]：ユーザ定義のフィルタを表示します。このダイアログボックスからユーザ定義のフィルタを編集または削除できます。 • [事前定義フィルタのリスト（List of pre-defined filters）]：システム定義のフィルタを表示します。 （注） [フィルタ（Filter）] アイコンを使用して、フィルタ フィールドを非表示または非表示解除できます。

表 *15* : *[システム イベント ログ（System Event Log）]* テーブル

名称	説明
[時刻（Time）] カラム	イベントが発生した日時。
[重大度（Severity）] カラム	重大度フィールドには、テキストと色分けされたアイコンの両方が含まれます。アイコンについては、緑色は通常動作、黄色は情報を示し、警告、クリティカルおよび回復不能なエラーは赤色で表示されます。
[説明（Description）] カラム	イベントの説明。

ロギング制御

ロギング制御の表示

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 [障害およびログ（Faults and Logs）] をクリックします。

ステップ 3 [ロギング制御（Logging Controls）] タブで、次の情報を確認します。

リモート ロギング

[名前（Name）]	説明
[有効化（Enable）] チェックボックス	オンにすると、Cisco IMC は [IP アドレス（IP Address）] フィールドで指定された Syslog サーバにログ メッセージを送信します。
[ホスト名/IP アドレス（Host Name/IP Address）] フィールド	Cisco IMC ログが保存される Syslog サーバのアドレス。リモート システムのアドレスとして IPv4 または IPv6 アドレスまたはドメイン名を設定できます。
[ポート（Port）] フィールド	1 ～ 65535 の範囲内の Syslog サーバの宛先ポート番号を入力します。デフォルトのポート番号は 514 です。

[名前（Name）]	説明
[プロトコル（Protocol）] フィールド	syslog メッセージ送信用のトランスポート層プロトコル。次のいずれかを選択できます。 • [TCP] • UDP
[リポートするための最小重大度（Minimum Severity to Report）] フィールド	リモート ログに含まれるメッセージの最低レベルを指定します。次のいずれかを選択できます。 • 緊急（Emergency） • アラート（Alert） • クリティカル（Critical） • エラー（Error） • 警告 • 通知（Notice） • 情報（Informational） • デバッグ（Debug）

（注） Cisco IMC では、選択した重大度よりも低い重大度のメッセージはリモートでログに記録されません。たとえば、[エラー（Error）] を選択した場合、Cisco IMC リモート ログには重大度が [緊急（Emergency）]、[アラート（Alert）]、[クリティカル（Critical）]、または [エラー（Error）] のすべてのメッセージが含まれます。[警告（Warning）]、[通知（Notice）]、[情報（Informational)]、または [デバッグ（Debug）] のメッセージは表示されません。

ローカル ロギング（Local Logging）

この領域には、上記の表に示すように [リポートするための最小重大度（Minimum Severity to Report）] ドロップダウンリストのみが表示されます。ローカル ログに含めるメッセージの最低レベルを指定できます。

次の作業

リモート サーバへの Cisco IMC ログの送信

Cisco IMC ログ エントリを受信するように 1 台または 2 台のリモート syslog サーバのプロファイルを設定できます。

はじめる前に

- リモート syslog サーバが、リモート ホストからのログを受信するよう設定されている必要があります。
- リモート syslog サーバが、authentication-related ログなどのすべてのタイプのログを受信するよう設定されている必要があります。
- リモート syslog サーバのファイアウォールが、syslog メッセージが syslog サーバに到達することを許可するよう設定されている必要があります。

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）] メニューの [障害およびログ（Faults and Logs）] をクリックします。

ステップ 3 [リモート Syslog サーバ（Remote Syslog Server）] 領域のいずれかで、次のフィールドに値を入力します。

[名前（Name）]	**説明**
[有効化（Enable）] チェックボックス	オンにすると、Cisco IMC は [IP アドレス（IP Address）] フィールドで指定された Syslog サーバにログ メッセージを送信します。
[ホスト名/IP アドレス（Host Name/IP Address）] フィールド	Cisco IMC ログが保存される Syslog サーバのアドレス。リモート システムのアドレスとして IPv4 または IPv6 アドレスまたはドメイン名を設定できます。
[ポート（Port）] フィールド	1 ～ 65535 の範囲内の Syslog サーバの宛先ポート番号を入力します。デフォルトのポート番号は 514 です。

ステップ 4 （任意） [リポートするための最小重大度（Minimum Severity to Report）] ドロップダウン リストで、リモート ログに含まれるメッセージの最低レベルを指定します。
次のいずれかを選択できます。重大度の高いものから順に並んでいます。

- 緊急（Emergency）
- アラート（Alert）
- クリティカル（Critical）
- エラー（Error）
- 警告
- 通知（Notice）
- 情報（Informational）

- デバッグ（Debug）

（注） Cisco IMC では、選択した重大度よりも低い重大度のメッセージは、リモートでログに記録されません。たとえば、[エラー（Error）] を選択した場合、Cisco IMC リモート ログには重大度が [緊急（Emergency）]、[アラート（Alert）]、[クリティカル（Critical）]、または [エラー（Error）] のすべてのメッセージが含まれます。[警告（Warning）]、[通知（Notice）]、[情報（Informational)]、または [デバッグ（Debug）] のメッセージは表示されません。

ステップ 5 [変更の保存（Save Changes）] をクリックします。

Cisco IMC ログしきい値の設定

はじめる前に

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 [障害およびログ（Faults and Logs）] をクリックします。

ステップ 3 [ローカル ロギング（Local Logging）] 領域で、[リポートするための最小重大度（Minimum Severity to Report）] ドロップダウン リストを使用して、Cisco IMC ログに含まれるメッセージの最低レベルを指定します。
次のいずれかを選択できます。重大度の高いものから順に並んでいます。

- 緊急（Emergency）
- アラート（Alert）
- クリティカル（Critical）
- エラー（Error）
- 警告
- 通知（Notice）
- 情報（Informational）
- デバッグ（Debug）

（注） Cisco IMC では、選択した重大度よりも低い重大度のメッセージはログに記録されません。たとえば、[エラー（Error）] を選択した場合、Cisco IMC ログには重大度が [緊急（Emergency）]、[アラート（Alert）]、[クリティカル（Critical）]、または [エラー（Error）] のすべてのメッセージが含まれます。[警告（Warning）]、[通知（Notice）]、[情報（Informational)]、または [デバッグ（Debug）] のメッセージは表示されません。

リモート サーバへのテスト Cisco IMC ログの送信

はじめる前に

- リモート syslog サーバが、リモート ホストからのログを受信するよう設定されている必要があります。
- リモート syslog サーバが、authentication-related ログなどのすべてのタイプのログを受信するよう設定されている必要があります。
- リモート syslog サーバのファイアウォールが、syslog メッセージが syslog サーバに到達することを許可するよう設定されている必要があります。

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）] メニューの [障害およびログ（Faults and Logs）] をクリックします。

ステップ 3 [障害およびログ（Faults and Logs）] ペインの [ロギング制御（Logging Controls）] タブをクリックします。

ステップ 4 [アクション（Action）] 領域の [テスト Syslog の送信（Send Test Syslog）] をクリックします。
設定されているリモート サーバにテスト Cisco IMC ログが送信されます。

第 17 章

サーバ ユーティリティ

この章の内容は、次のとおりです。

テクニカル サポート データのエクスポート

テクニカル サポート データのエクスポート

このタスクは、Cisco Technical Assistance Center（TAC）から要求された場合に実行します。このユーティリティは、TAC が技術上の問題をトラブルシューティングおよび解決する際に役立つ設定情報、ログ、および診断データが含まれる要約レポートを作成します。

手順

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

ステップ 2 [管理者（Admin）] メニューの [ユーティリティ（Utilities）] をクリックします。

ステップ 3 [ユーティリティ（Utilities）] ペインの [アクション（Actions）] 領域で、[テクニカルサポートデータのエクスポート（Export Technical Support Data）] をクリックします。

ステップ 4 [テクニカル サポート データのエクスポート（Export Technical Support Data）] ダイアログボックスで、次のフィールドに入力します。

[名前（Name）]	説明
[テクニカル サポート データのエクスポート先（Export Technical Support Data through）] ドロップダウン リスト	（注） [前面パネルの USB（Front Panel USB）] オプションは、[スマート アクセス USB（Smart Access USB）] が有効になっており、USB ストレージ デバイスがサーバに接続されている場合にのみ表示されます。 テクニカル サポート データをリモート サーバ、またはサーバに接続している USB ストレージ デバイスにエクスポートできます。次のいずれかを選択できます。 • [リモート（Remote）]：次のいずれかのプロトコルを使用して、リモート サーバにテクニカル サポート データをエクスポートできます。 ◦ TFTP ◦ FTP ◦ SFTP ◦ SCP ◦ HTTP （注） このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「サーバ（*RSA*）キー 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?*）」というメッセージとともにポップアップ ウィンドウが表示されます。サーバ フィンガープリントの信頼性に応じて、[はい（Yes）] または [いいえ（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に基づいており、接続先のホストを識別または確認できます。 • [前面パネルの USB（Front Panel USB）]：サーバに接続している USB ストレージ デバイスにテクニカル サポート データをエクスポートできます。
[サーバ IP/ホスト名（Server IP/Hostname）] フィールド	サポート データ ファイルを保存する必要のあるサーバの IP アドレスまたはホスト名。[テクニカル サポート データのエクスポート先（Export Technical Support Data to）] 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（Name）]	説明
[パスおよびファイル名（Path and Filename）] フィールド	ファイルをリモート サーバにエクスポートするときに、Cisco IMC で使用するパスおよびファイル名。 （注） サーバにサポート対象ネットワーク アダプタ カードのいずれかがある場合、データ ファイルにはアダプタ カードからのテクニカル サポート データも含まれています。
[ユーザ名（Username）]	システムがリモート サーバへのログインに使用する必要のあるユーザ名。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。
[パスワード（Password）]	リモート サーバのユーザ名のパスワード。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。

ステップ 5 [エクスポート（Export）] をクリックします。

次の作業

生成されたレポート ファイルを Cisco TAC に提供します。

ローカル ファイルへのテクニカル サポート データのダウンロード

このタスクは、Cisco Technical Assistance Center（TAC）から要求された場合に実行します。このユーティリティは、TAC が技術上の問題をトラブルシューティングおよび解決する際に役立つ設定情報、ログ、および診断データが含まれる要約レポートを作成します。

手順

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

ステップ 2 [管理者（Admin）] メニューの [ユーティリティ（Utilities）] をクリックします。

ステップ 3 [ユーティリティ（Utilities）] ペインの [アクション（Actions）] 領域で、[ローカル ダウンロード用のテクニカル サポート データの作成（Generate Technical Support Data for Local Download）] をクリックします。

ステップ 4 [ローカル ファイルへのテクニカル サポート データのダウンロード（Download Technical Support Data to Local File）] ダイアログボックスで、次のフィールドに入力します。

[名前（Name）]	説明
[テクニカル サポート データの作成（Generate Technical Support Data）] オプション ボタン	Cisco IMC ダウンロードするテクニカル サポート データ ファイルがない場合、このオプション ボタンは無効化されます。 [生成（Generate）] をクリックして、データ ファイルを作成します。データ収集が完了したら、[アクション（Actions）] 領域の [ローカル ファイルへのテクニカル サポート データのダウンロード（Download Technical Support Data to Local File）] をクリックして、ファイルをダウンロードします。
[テクニカル サポート データの再作成（Regenerate Technical Support Data）] オプション ボタン	Cisco IMC テクニカル サポート データ ファイルがダウンロード可能な場合、このオプション ボタンが表示されます。 既存のサポート データ ファイルを新しいものと置き換えるには、このオプションを選択し、[再作成（Regenerate）] をクリックします。データ収集が完了したら、[アクション（Actions）] 領域の [ローカル ファイルへのテクニカル サポート データのダウンロード（Download Technical Support Data to Local File）] をクリックして、ファイルをダウンロードします。
[ローカル ファイルへダウンロード（Download to local file）] オプション ボタン	Cisco IMC テクニカル サポート データ ファイルがダウンロード可能な場合、このオプション ボタンが有効になります。 既存のファイルをダウンロードするには、このオプションを選択し、[ダウンロード（Download）] をクリックします。 （注） サーバにサポート対象ネットワーク アダプタ カードのいずれかがある場合、データ ファイルにはアダプタ カードからのテクニカル サポート データも含まれています。
[作成およびダウンロード（Generate and Download）] ボタン	テクニカル サポート データ ファイルを作成してダウンロードできます。
[生成（Generate）] ボタン	テクニカル サポート データ ファイルを作成できます。
[ダウンロード（Download）] ボタン	テクニカル サポート データ ファイルを作成後にダウンロードできます。

ステップ 5 [生成（Generate）] をクリックして、データ ファイルを作成します。データ収集が完了したら、[アクション（Actions）] 領域の [ローカル ファイルへのテクニカル サポート データのダウンロード（Download Technical Support Data to Local File）] をクリックして、ファイルをダウンロードします。

次の作業

生成されたレポート ファイルを Cisco TAC に提供します。

出荷時の初期状態へのリセット

非常に稀なケースですが、現在稼動しているファームウェアで問題が発生した場合やサーバのトラブルシューティング時などに、サーバ コンポーネントの出荷時デフォルトへのリセットが必要になることがあります。これを行うと、ユーザが設定可能なすべての設定がリセットされます。

この手順は、通常のサーバメンテナンスには含まれません。サーバコンポーネントをリセットした後は、ログオフしてから再びログインする必要があります。また、接続が失われ、ネットワーク設定の再指定が必要になる場合もあります。この移行中、一部のインベントリ情報が使用できないことがあります。

BMC を工場出荷時の設定にリセットすると、シリアル番号が Cisco IMCXXXXXX 形式で表示されます。XXXXXX はサーバのシリアル番号です。

重要 VIC アダプタを他の世代の C シリーズ サーバ（たとえば M4）から M5 世代の C シリーズ サーバまたは M5 サーバから他の世代のサーバに移動する際は、アダプタを出荷時のデフォルトにリセットする必要があります。

はじめる前に

サーバ コンポーネントを出荷時デフォルトにリセットするには、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 [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [ユーティリティ（Utilities）] をクリックします。

ステップ 3 [ユーティリティ（Utilities）] ペインの [アクション（Actions）] 領域で、[工場出荷時のデフォルトにリセット（Reset to Factory Default）] をクリックします。

ステップ 4 [工場出荷時のデフォルトにリセット（Reset to Factory Default）] ダイアログボックスで、次の情報を確認します。

名称	説明
[すべて（All）] チェックボックス	オンにすると、サーバのすべてのコンポーネントが工場出荷時の設定にリセットされます。 展開して、工場出荷時の設定にリセットする特定のコンポーネントを選択します。

名称	説明
[BMC] チェックボックス	オンにすると、BMC が工場出荷時の設定にリセットされます。 （注） BMC を工場出荷時の設定にリセットすると、シリアル番号が Cisco IMCXXXXXX 形式で表示されます。XXXXXX はサーバのシリアル番号です。また、リセット時には、デフォルトで Cisco Card モードが設定されます。
[ストレージ（Storage）] チェックボックス	オンにすると、使用可能なすべてのストレージアダプタが工場出荷時の設定にリセットされます。ストレージ アダプタをリセットすると、ディスク上のデータは変更されませんが、仮想ドライブのメタデータは消去され、データ損失が発生することがあります。展開して、工場出荷時の設定にリセットする特定のストレージ アダプタを選択します。 （注） ストレージ アダプタを工場出荷時の設定にリセットするには、ホストの電源がオンになっている必要があります。
[VIC] チェックボックス	オンにすると、使用可能なすべての VIC が工場出荷時の設定にリセットされます。 展開して、工場出荷時の設定にリセットする特定の VIC を選択します。 （注） VIC を工場出荷時の設定にリセットするには、ホストの電源がオンになっている必要があります。
[リセット（Reset）] ボタン	選択したコンポーネントが工場出荷時の設定にリセットされます。

ステップ 5 [リセット（Reset）] をクリックして、選択したコンポーネントを工場出荷時の設定にリセットします。

ホストが BIOS POST（電源投入時自己診断テスト）を実行しているとき、または EFI シェル内にあるときに、Cisco IMC を再起動するとホストの電源が短時間オフになります。準備ができると、Cisco IMC の電源はオンになります。再起動時に、ネットワーク設定モードはデフォルトで [シスコ カード（Cisco Card）] モードに設定されます。

Cisco IMC 設定のエクスポートとインポート

Cisco IMC 設定のエクスポートとインポート

Cisco IMC 設定のバックアップを実行するには、システム設定のスナップショットを作成し、生成された Cisco IMC 設定ファイルをネットワーク上の場所にエクスポートします。エクスポート操作で保存されるのは、管理プレーンからの情報だけです。サーバ上のデータはバックアップされません。ユーザ アカウントやサーバ証明書など、機密情報の設定はエクスポートされません。

エクスポートされた Cisco IMC 設定ファイルは、同じシステムで復元したり、別の Cisco IMC システムにインポートしたりできます。ただし、インポートするシステムのソフトウェアのバージョンとエクスポートするシステムのソフトウェアのバージョンが同じであるか、両者の設定に互換性があることが前提となります。設定ファイルを設定テンプレートとして他のシステムにインポートする場合は、IP アドレスやホスト名などシステム固有の設定を変更する必要があります。インポート操作によって情報が変更されるのは、管理プレーンだけです。

Cisco IMC 設定ファイルは XML テキスト ファイルで、その構造と要素は Cisco IMC コマンド モードに対応しています。

エクスポートまたはインポート操作を実行する場合は、次のガイドラインを考慮してください。

- エクスポートまたはインポートは、システムがアップ状態で、稼働しているときに実行できます。エクスポート操作によるサーバまたはネットワーク トラフィックへの影響はありませんが、インポート操作によって IP アドレスなどが変更されると、トラフィックが中断されたりサーバがリブートされたりすることがあります。
- エクスポートとインポートを同時に実行することはできません。

次の機能でインポートまたはエクスポート操作を実行できます。

- Cisco IMC バージョン

（注） この情報のみをエクスポートできます。

- ネットワーク設定（Network settings）
- テクニカル サポート
- ローカル ログおよびリモート ログのロギング制御
- 電力ポリシー
- BIOS - BIOS パラメータ

（注） 高精度ブートはサポートされません。

- コミュニケーション サービス
- リモート プレゼンス
- ユーザ管理 - LDAP
- イベント管理
- SNMP
- ダイナミック ストレージの設定
- シャーシの説明

Cisco IMC 設定のエクスポート

（注） セキュリティ上の理由から、この操作ではユーザ アカウントやサーバ証明書はエクスポートされません。

はじめる前に

バックアップ リモート サーバの IP アドレスを取得します。

手順

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

ステップ 2 [管理者（Admin）] メニューの [ユーティリティ（Utilities）] をクリックします。

ステップ 3 [ユーティリティ（Utilities）]ペインの [アクション（Actions）] 領域で、[エクスポート設定（Export Configuration）] をクリックします。

ステップ 4 [エクスポート設定（Export Configuration）] ダイアログボックスで、次のフィールドに値を入力します。

名称	説明
[エクスポート用コンポーネントの選択（Select Component for Export）] ドロップダウン リスト	コンポーネント タイプ。次のいずれかになります。 • BMC • VIC アダプタ 選択したコンポーネントに応じて、そのコンポーネントの設定がエクスポートされます。

名称	説明
[エクスポート先（Export To）] ドロップダウン リスト	XML 設定ファイルを保存する場所。次のいずれかになります。 • [ローカル（Local）]：Cisco IMC GUI を実行しているコンピュータのローカル ドライブに XML 設定ファイルを保存するには、このオプションを選択して [エクスポート（Export）] をクリックします。 このオプションを選択すると、Cisco IMC GUI に [ファイルのダウンロード（File Download）] ダイアログボックスが表示され、設定ファイルを保存する場所に移動できます。 • [リモート サーバ（Remote Server）]：XML 設定ファイルをリモート サーバからインポートするには、このオプションを選択します。 このオプションを選択すると、Cisco IMC GUI にリモート サーバのフィールドが表示されます。 • [前面パネルの USB（Front Panel USB）]：サーバに接続していUSBストレージデバイスに設定ファイルをエクスポートするには、このオプションを選択します。 （注） • Cisco IMC の設定をエクスポートするための [前面パネルの USB（Front Panel USB）] オプションは、[スマート アクセス USB（Smart Access USB）] が有効になっており、USB ストレージ デバイスがサーバに接続されている場合にのみ使用できます。 • このオプションは、[コンポーネントの選択（Select Component）] ドロップダウン リストで [BMC] を選択した場合にのみ使用できます。

名称	説明
[エクスポート先（Export To）] ドロップダウン リスト	リモート サーバのタイプ。次のいずれかになります。 • TFTP サーバ（TFTP Server） • FTP サーバ（FTP Server） • SFTP サーバ（SFTP Server） • SCP サーバ • HTTP サーバ（HTTP Server） （注） このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「サーバ（*RSA*）キー 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?*）」というメッセージとともにポップアップ ウィンドウが表示されます。サーバ フィンガープリントの信頼性に応じて、[はい（Yes）] または [いいえ（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に基づいており、接続先のホストを識別または確認できます。
[サーバ IP/ホスト名（Server IP/Hostname）] フィールド	設定ファイルのエクスポート先となるサーバの IPv4 アドレスか IPv6 アドレス、またはホスト名。[エクスポート先（Export to）] ドロップダウン リストで選択したリモート サーバのタイプに応じて、フィールド名が異なることがあります。
[パスおよびファイル名（Path and Filename）] フィールド	ファイルをリモート サーバにエクスポートするときに、Cisco IMC で使用するパスおよびファイル名。
[ユーザ名（Username）]	システムがリモート サーバへのログインに使用する必要のあるユーザ名。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。
[パスワード（Password）]	リモート サーバのユーザ名のパスワード。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。
[パスフレーズ（Passphrase）]	エクスポートした設定ファイル内の LDAP および SNMP v3 ユーザ パスワードの暗号化に AES256 アルゴリズムを使用するパスフレーズ。6 ～ 127 文字の文字列を入力します。次の文字は入力しないでください：! # $ & < > ? ; ' | ` ~ \ % ^ ( )"

ステップ 5 [エクスポート（Export）] をクリックします。

Cisco IMC 設定のインポート

はじめる前に

設定ファイルをインポートするときに SNMP 設定情報を復元する必要がある場合は、インポートを実行する前に、このサーバで SNMP がディセーブルになっていることを確認します。インポートを実行するときに SNMP がイネーブルになっている場合、Cisco IMC では設定ファイルに保存されている値によって現在の値は上書きされません。

手順

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

ステップ 2 [管理者（Admin）] メニューの [ユーティリティ（Utilities）] をクリックします。

ステップ 3 [ユーティリティ（Utilities）] ペインの [アクション（Actions）] 領域で、[インポート設定（Import Configuration）] をクリックします。

ステップ 4 [インポート設定（Import Configuration）] ダイアログボックスで、次のフィールドに値を入力します。

名称	説明
[インポート用コンポーネントの選択（Select Component for Import）] ドロップダウン リスト	コンポーネント タイプ。次のいずれかになります。 • BMC • VIC アダプタ 選択したコンポーネントに応じて、そのコンポーネントの設定がインポートされます。

名称	説明
[インポート元（Import From）] ドロップダウン リスト	XML 設定ファイルの場所。次のいずれかになります。 • [ローカル（Local）]：Cisco IMC GUI を実行しているコンピュータのローカル ドライブに XML 設定ファイルをインポートするには、このオプションを選択します。 このオプションを選択すると、Cisco IMC GUI に [参照（Browse）] ボタンが表示され、インポートするファイルに移動できます。 • [リモート サーバ（Remote Server）]：XML 設定ファイルをリモート サーバからインポートするには、このオプションを選択します。 このオプションを選択すると、Cisco IMC GUI にリモート サーバのフィールドが表示されます。 • [前面パネルの USB（Front Panel USB）]：サーバに接続していUSBストレージデバイスから設定ファイルをインポートするには、このオプションを選択します。 （注） • Cisco IMC の設定をインポートするための [前面パネルの USB（Front Panel USB）] オプションは、[スマート アクセス USB（Smart Access USB）] が有効になっており、USB ストレージ デバイスがサーバに接続されている場合にのみ使用できます。 • このオプションは、[コンポーネントの選択（Select Component）] ドロップダウン リストで [BMC] を選択した場合にのみ使用できます。

名称	説明
[インポート元（Import From）] ドロップダウン リスト	（注） これらのオプションは、[リモート（Remote）] を選択した場合にのみ使用できます。 リモート サーバのタイプ。次のいずれかになります。 • TFTP サーバ（TFTP Server） • FTP サーバ（FTP Server） • SFTP サーバ（SFTP Server） • SCP サーバ • HTTP サーバ（HTTP Server） （注） このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「サーバ（*RSA*）キー 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?*）」というメッセージとともにポップアップ ウィンドウが表示されます。サーバフィンガープリントの信頼性に応じて、[はい（Yes）] または [いいえ（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に基づいており、接続先のホストを識別または確認できます。
[サーバ IP/ホスト名（Server IP/Hostname）] フィールド	設定ファイルが存在するサーバの IPv4 アドレスか IPv6 アドレス、またはホスト名。[インポート元（Import From）] ドロップダウン リストで選択したリモート サーバのタイプに応じて、フィールド名が異なることがあります。
[パスおよびファイル名（Path and Filename）] フィールド	リモート サーバ上の設定ファイルのパスおよびファイル名。
[ユーザ名（Username）]	システムがリモート サーバへのログインに使用する必要のあるユーザ名。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。
[パスワード（Password）]	リモート サーバのユーザ名のパスワード。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。

名称	説明
パスフレーズ（Passphrase）	インポートした設定ファイル内の LDAP および SNMP v3 ユーザ パスワードの暗号化に AES256 アルゴリズムを使用するパスフレーズ。6 ～ 127 文字の文字列を入力します。次の文字は入力しないでください : ! # $ & < > ? ; ' | ` ~ \ % ^ ( ) " （注） 設定ファイルの暗号化されたセクションを編集しそれをインポートしようとすると、編集内容は無視され、インポート操作画面には部分的な成功メッセージが表示されます。

ステップ 5 [インポート（Import）] をクリックします。

ホストへのマスク不能割り込みの生成

状況によっては、サーバがハングして、従来のデバッグ メカニズムに応答しない場合があります。ホストへのマスク不能割り込み（NMI）を生成することにより、サーバのクラッシュ ダンプ ファイルを作成および送信して、サーバのデバッグに使用することができます。

サーバに関連付けられたオペレーティング システムの種類によっては、このタスクで OS が再起動される場合があります。

はじめる前に

- 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。
- サーバの電源をオンに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 [管理者（Admin）] メニューをクリックします。

ステップ 2 [管理者（Admin）] メニューの [ユーティリティ（Utilities）] をクリックします。

ステップ 3 [ユーティリティ（Utilities）] ペインの [アクション（Actions）] 領域で、[NMI をホストに作成（Generate NMI to Host）] をクリックします。

ステップ 4 [NMI をホストに作成（Generate NMI to Host）] ダイアログボックスで、次の情報を確認します。

アクション（Actions）	説明
[NMI の作成先（Generate NMI to）] ドロップダウン リスト	マスク不能割り込み（NMI）を生成するサーバを選択できます。次のいずれかになります。 • [サーバ 1（Server 1）] • サーバ 2

ステップ 5 [送信（Send）] をクリックします。
このアクションは、OS を再起動する可能性のあるホストに NMI 信号を送信します。

Cisco IMC バナーの追加または更新

著作権表記やカスタマイズされたメッセージなどの重要な情報を入力して、Cisco IMC バナーを追加または更新できます。次の手順を実行します。

はじめる前に

手順

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

ステップ 2 [管理者（Admin）] メニューの [ユーティリティ（Utilities）] をクリックします。

ステップ 3 [ユーティリティ（Utilities）] ペインの [アクション（Actions）] 領域で、[Cisco IMC バナーの追加/更新（Add/Update Cisco IMC Banner）] をクリックします。

ステップ 4 [Cisco IMC バナーの追加/更新（Add/Update Cisco IMC Banner）] ダイアログボックスで、次のフィールドに値を入力します。

[名前（Name）]	説明
[バナー（1 行あたり 80 文字。最大 2K 文字。）（Banner (80 Chars per line.Max 2K Chars.)）] フィールド	Web UI またはコマンドライン インターフェイスにログインする前に、ログイン画面に表示する著作権情報またはメッセージを入力します。
[SSH の再起動（Restart SSH）] チェックボックス	オンにすると、[バナーの保存（Save Banner）] ボタンをクリックした後にアクティブな SSH セッションが終了します。

ステップ 5 [バナーの保存（Save Banner）] をクリックします。

次の作業

Cisco IMC の最後のリセット理由の表示

手順

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

ステップ 2 [管理者（Admin）] メニューの [ユーティリティ（Utilities）] をクリックします。

ステップ 3 [ユーティリティ（Utilities）]ペインの[アクション（Actions）]領域で、[最後のリセット理由（Last Reset Reason）] 領域の下にある次の情報を確認します。

[名前（Name）]	**説明**
[コンポーネント（Component）] フィールド	最後にリセットされたコンポーネント。
[ステータス（Status）] フィールド	コンポーネントが最後にリセットされた理由。次のいずれかになります。 • [ウォッチドッグによるリセット（watchdog-reset）]：Cisco IMC のメモリが容量一杯に到達した時点でウォッチドッグタイマーがリセットします。 • [ac サイクル（ac-cycle）]：PSU 電源ケーブルが取り外されています（電源入力なし）。 • [グレースフル リブート（graceful-reboot）]：Cisco IMC のリブートが実行されます。

ローカルファイルへのハードウェアインベントリのダウンロード

手順

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

ステップ 2 [管理者（Admin）] メニューの [ユーティリティ（Utilities）] をクリックします。

ステップ 3 [ユーティリティ（Utilities）] ペインの [アクション（Actions）] 領域で、[インベントリ データの生成（Generate Inventory Data）] をクリックします。

ステップ 4 [インベントリ データの生成（Generate Inventory Data）] ダイアログ ボックスで、次のフィールドに値を入力します。

[名前（Name）]	説明
[インベントリ データの生成（Generate Inventory Data）] オプション ボタン	Cisco IMC ダウンロードするハードウェア インベントリ データ ファイルがない場合、このオプション ボタンが表示されます。
[ローカル ファイルへダウンロード（Download to local file）] オプション ボタン	Cisco IMC インベントリ データ ファイルがダウンロード可能な場合、このオプション ボタンが有効になります。 既存のファイルをダウンロードするには、このオプションを選択し、[ダウンロード（Download）] をクリックします。

ステップ 5 [生成（Generate）] をクリックして、データ ファイルを作成します。データ収集が完了したら、[ローカル ファイルへのインベントリ データのダウンロード（Download Inventory Data to Local File）] オプション ボタンを選択して [ダウンロード（Download）] をクリックし、ファイルをローカルにダウンロードします。

リモート サーバへのハードウェア インベントリ データのエクスポート

手順

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

ステップ 2 [管理者（Admin）] メニューの [ユーティリティ（Utilities）] をクリックします。

ステップ 3 [ユーティリティ（Utilities）] ペインの [アクション（Actions）] 領域で、[リモートへのハードウェア インベントリ データのエクスポート（Export Hardware Inventory Data to Remote）] をクリックします。

ステップ 4 [ハードウェア インベントリ データのエクスポート（Export Hardware Inventory Data）] ダイアログ ボックスで、次のフィールドに値を入力します。

[名前（Name）]	説明
[ハードウェア インベントリ データのエクスポート先（Export Hardware Inventory Data to）] ドロップダウン リスト	リモート サーバのタイプ。次のいずれかになります。 • TFTP サーバ（TFTP Server） • FTP サーバ（FTP Server） • SFTP サーバ（SFTP Server） • SCP サーバ • HTTP サーバ（HTTP Server） （注） このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「サーバ（*RSA*）キー 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?*）」というメッセージとともにポップアップ ウィンドウが表示されます。サーバ フィンガープリントの信頼性に応じて、[はい（Yes）] または [いいえ（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に基づいており、接続先のホストを識別または確認できます。
[サーバIP/ホスト名（Server IP/Hostname）] フィールド	データ ファイルを保存する必要のあるサーバの IP アドレスまたはホスト名。[ハードウェア インベントリ データのエクスポート先（Export Hardware Inventory Data to）] 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（Name）]	説明
[パスおよびファイル名（Path and Filename）] フィールド	ファイルをリモート サーバにエクスポートするときに、Cisco IMC で使用するパスおよびファイル名。
[ユーザ名（Username）]	システムがリモート サーバへのログインに使用する必要のあるユーザ名。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。
[パスワード（Password）]	リモート サーバのユーザ名のパスワード。このフィールドは、プロトコルが TFTP または HTTP の場合は適用されません。

ステップ 5 [エクスポート（Export）] をクリックします。

PID カタログのアップロード

はじめる前に

PID カタログをアップロードするには、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 [管理者（Admin）] タブをクリックします。

ステップ 2 [管理者（Admin）] タブの[ユーティリティ（Utilities）] をクリックします。

ステップ 3 [作業（Work）] ペインで [PID カタログのアップロード（Upload PID Catalog）] リンクをクリックします。
[PID カタログのアップロード（Upload PID Catalog）] ダイアログボックスが表示されます。

カタログ ファイルが保管されている場所に応じて、次のいずれかのオプションを選択します。

ステップ 4 [ローカル ファイルからの PID カタログのアップロード（Upload PID Catalog from Local File）] ダイアログボックスで[参照（Browse）] をクリックし、[アップロードするファイルを選択（Choose File to Upload）] ダイアログボックスを使用してアップロードするカタログ ファイルを選択します。

[名前（Name）]	説明
[ファイル（File）] フィールド	アップロードする PID カタログ ファイル。
[参照（Browse）] ボタン	該当するファイルに移動するためのダイアログボックスが開きます。

ステップ 5 [リモート サーバからの PID カタログのアップロード（Upload PID Catalog from Remote Server）] ダイアログボックスで、次のフィールドに値を入力します。

[名前（Name）]	**説明**
[リモート サーバからの PID カタログのアップロード（Upload PID Catalog from Remote Server）] ドロップダウンリスト	リモート サーバのタイプ。次のいずれかになります。 • TFTP • FTP • SFTP • SCP • HTTP
[サーバIP/ホスト名（Server IP/Hostname）] フィールド	PID カタログ情報を有効にするサーバの IP アドレスまたはホスト名。[PID カタログのアップロード元（Upload PID Catalog 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。
[パスおよびファイル名（Path and Filename）] フィールド	リモート サーバ上のカタログ 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。

[名前（Name）]	説明
[アップロード（Upload）] ボタン	選択した PID カタログがアップロードされます。 （注） このアクションを実行しながら、リモート サーバ タイプとして SCP または SFTP を選択した場合、「サーバ（*RSA*）キー 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?*）」というメッセージとともにポップアップ ウィンドウが表示されます。サーバ フィンガープリントの信頼性に応じて、[はい（Yes）] または [いいえ（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に基づいており、接続先のホストを識別または確認できます。
[キャンセル（Cancel）] ボタン	サーバに保存されたファームウェア バージョンを変更せずにウィザードを終了します。

PID カタログの有効化

はじめる前に

PID カタログを有効にするには、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 [管理者（Admin）] タブをクリックします。

ステップ 2 [管理者（Admin）] タブの[ユーティリティ（Utilities）] をクリックします。

ステップ 3 [作業（Work）] ペインで [PID カタログの有効化（Activate PID Catalog）] リンクをクリックします。

[PID カタログの有効化（Activate PID Catalog）] ダイアログボックスが表示されます。次のフィールドに入力します。

[名前（Name）]	説明
[アクティブ化（Activate）] ボタン	PID カタログをアクティブにできます。

（注） 初めてシステムにログインしている場合は、[PID カタログの有効化（Activate PID Catalog）] リンクは無効になっています。PID カタログをサーバにアップロードすると、このリンクが有効になります。PID ファイルをアップロードした後はリンクが有効な状態で維持されるので、PID を何度でもアクティブにすることができます。

スマート アクセス USB の有効化

スマート アクセス USB 機能を有効にすると、フロント パネルの USB デバイスはホスト オペレーティング システムから切断され、Cisco IMC に接続します。スマート アクセス USB 機能を有効にした後は、フロントパネルの USB デバイスを使用して、テクニカル サポート データをエクスポート、Cisco IMC 構成をインポートまたはエクスポート、あるいは Cisco IMC、BIOS および VIC のファームウェアを更新できます。
スマート アクセス USB でサポートされるファイル システムは次のとおりです。

- EXT2
- EXT3
- EXT4
- FAT 32
- FAT 16
- DoS

（注） 巨大ファイル サポートは BMC ではサポートされません。EXT4 ファイルシステムの場合、巨大ファイルのサポートをオフにする必要があります。

はじめる前に

このタスクを実行するには、admin 権限で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 [管理者（Admin）] タブをクリックします。

ステップ 2 [管理者（Admin）] メニューの [ユーティリティ（Utilities）] をクリックします。

ステップ 3 [アクション（Actions）] 領域で [スマートアクセスUSBの有効化（Enable Smart Access USB）] をクリックします。
これはトグル ボタンです。スマート アクセスを無効にするには、[スマートアクセスUSBの無効化（Disable Smart Access USB）] をクリックします。スマート アクセス USB を有効にした後にのみ、このボタンが表示されます。スマート アクセス USB 機能を無効にすると、フロント パネルの USB デバイスは Cisco IMC から切断してホスト オペレーティング システムに接続します。

Starship 管理の有効化と無効化

Starship 管理を有効にすると、Starship クラウド アプリケーションと M5 サーバ間の双方向通信が確立されます。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理者（Admin）] タブをクリックします。

ステップ 2 [管理者（Admin）] タブの [デバイスコネクタ（Device Connector）] をクリックします。

ステップ 3 [Starship管理（Starship Management）] エリアで、[オン（On）] をクリックして Starship の管理を有効にします。
[接続（Connection）] エリアに Starship 管理の接続状態が表示されます。デバイス コネクタの Starship 管理への接続が確立できていない場合は、[詳細と推奨事項（Details & Recommendations）] ドロップダウン リストに表示される推奨事項を確認し、接続の問題を修正します。

ステップ 4 Starship 管理を無効にするには、[オフ（Off）] をクリックします。
Starship 管理を無効にすると、[接続（Connection）] エリアに接続状態が [管理上無効（Administratively Disabled）] として表示されます。

デバイス コネクタの HTTPS プロキシ設定の設定

サーバの HTTPS プロキシ設定を手動で構成できます。

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理者（Admin）] タブをクリックします。

ステップ 2 [管理者（Admin）] タブの [デバイスコネクタ（Device Connector）] をクリックします。

ステップ 3 [接続（Connections）] エリアで、[HTTPSプロキシ設定（HTTPS Proxy Settings）] をクリックしてプロキシ設定を入力します。

アクション名	説明
[オフ（Off）] ボタン	HTTPS プロキシ設定を無効にします。
[手動（Manual）] ボタン	HTTPS プロキシ設定を手動で構成できます。
[プロキシホスト名/IP（Proxy Hostname/IP）] フィールド	プロキシサーバの IP アドレスまたはホスト名。
[プロキシポート（Proxy Port）] フィールド	プロキシ サーバのポート番号。
[認証（Authentication）] トグル ボタン	このオプションを有効にすると、プロキシサーバのクレデンシャルを提供できます。
[ユーザ名（Username）] フィールド	プロキシ サーバのクレデンシャルです。
[パスワード（Password）] フィールド	

ステップ 4 [HTTPSプロキシ設定（HTTPS Proxy Settings）] ダイアログ ボックスで、情報を追加してから [保存（Save）] をクリックします。

Starship デバイス コネクタのプロパティの表示

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [管理者（Admin）] タブをクリックします。

ステップ 2 [管理者（Admin）] タブの [デバイスコネクタ（Device Connector）] をクリックします。

ステップ 3 [Starship管理（Starship Management）] 領域で、次の情報を確認します。

アクション名	説明
[状態（State）] オプション ボタン	Starship 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。 • [オン（On）]：Starship 管理を有効にします。 • [オフ（Off）]：Starship 管理を無効にします。

ステップ 4 [接続（Connection）] 領域で、次の情報を確認します。

名称	説明
[ステータス（Status）] フィールド	Starship への接続の状態を表示します。次のいずれかになります。 • [管理上無効（Administratively Disabled）]：Starship の管理が無効になっていることを示します。 • [DNS誤設定（DNS Misconfigured）]：BMC で DNS の詳細が設定されていないことを示します。 • [UCS接続ネットワークエラー（UCS Connect Network Error）]：無効なネットワーク構成を示します。 • [証明書検証エラー（Certification Validation Error）]：無効な証明書を示します。 • [要求あり（Claimed）]：Starship でデバイスが要求されていることを示します。 • [要求なし（Not Claimed）]Starship でデバイスが登録されましたが、要求されていないことを示します。
[接続再試行（Retry Connection）] リンク	Starship への接続を再試行できます。このオプションは、Starship の接続に問題がある場合のみに表示されます。
[詳細と推奨事項（Details & Recommendations）] ドロップダウン リスト	状態に基づいて接続の問題を修正するための詳細と推奨事項を表示します。

名称	説明
[HTTPSプロキシ設定（HTTPS Proxy Settings）] ダイアログ ボックス	Starship 接続に必要な HTTPS プロキシ設定を手動で構成できます。
[シリアル番号（Serial Number）] フィールド	BMC のシリアル番号を表示します。
[セキュリティトークン（Security Token）] フィールド	接続ステータスが [要求なし（Not Claimed）] の場合に表示されます。Starship にサーバを安全に搭載するにはセキュリティ トークンを使用します。

ステップ 5 [接続（Connections）] エリアで、[HTTPSプロキシ設定（HTTPS Proxy Settings）] をクリックして次の情報を確認します。

アクション名	説明
[オフ（Off）] ボタン	HTTPS プロキシ設定を無効にします。
[手動（Manual）] ボタン	HTTPS プロキシ設定を手動で構成できます。
[プロキシホスト名/IP（Proxy Hostname/IP）] フィールド	プロキシ サーバの IP アドレスまたはホスト名。
[プロキシポート（Proxy Port）] フィールド	プロキシ サーバのポート番号。
[認証（Authentication）] トグル ボタン	このオプションを有効にすると、プロキシサーバのクレデンシャルを提供できます。
[ユーザ名（Username）] フィールド	プロキシ サーバのクレデンシャルです。
[パスワード（Password）] フィールド	

第 18 章

トラブルシューティング

この章の内容は、次のとおりです。

最後の起動プロセスの記録

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 作業ウィンドウの [トラブルシューティング（TroubleShooting）] タブをクリックします。

ステップ 3 [トラブルシューティング（Troubleshooting）] タブの [ブートストラップ処理の記録（Bootstrap Process Recording）] 領域で、[記録の有効化（Enable Recording）] チェックボックスをオンにします。

デフォルトで、このオプションは有効になっています。

注意 このタスクはトラブルシューティング目的のもので、常に有効にしていると Cisco IMC パフォーマンスに影響する場合があります。

ステップ 4 （任意） BIOS POST するまで起動プロセスを記録する場合は、[BIOS POST 時に停止（Stop On BIOS POST）] チェックボックスをオンにします。

ステップ 5 [変更内容を保存（Save Changes）] をクリックします。

ステップ 6 [作業（Work）] ペイン上部のツールバーで、[サーバの電源オン（Power On Server）] をクリックします。

ステップ 7 [ブートストラップ処理の記録（Bootstrap Process Recording）] ペインの [アクション（Actions）] 領域で、[メッセージを再生する（Play Recording）] をクリックします。
サポートされている Java バージョンに関する手順を示した確認ダイアログボックスが表示されます。

ステップ 8 手順を確認し、[OK] をクリックします。
[DVR Player のコントロール（DVR Player Controls）] ダイアログボックスが開きます。このダイアログボックスは、最後の起動プロセスの記録を再生します。[BIOS POST 時に停止（Stop On BIOS POST）] オプションをイネーブルにしている場合は、システムは BIOS POST まで記録プロセスを再生します。

この記録を確認して、システムがリブートした要因を分析できます。

ステップ 9 [ブートストラップ処理の記録（Bootstrap Process Recording）] 領域の [アクション（Actions）] 領域で、[記録のダウンロード（Download Recording）] をクリックします。
ダウンロードするには、手順に従ってください。

（注） ファイルがローカル ドライブに `.dvc` 形式で保存されます。KVM プレーヤーまたはオフライン プレーヤーを使用してこの記録を表示できます。[記録のダウンロード（Download Recording）] オプションを選択するたびに、最後の起動プロセスが記録され、ファイル名が自動生成され、事前に指定されたパスに保存されます。

ステップ 10 ダウンロードが完了すると、記録のビデオを再生するファイルを選択できるので、選択して [開く（Open）] をクリックします。
[DVR Player のコントロール（DVR Player Controls）] ウィンドウが開き、選択したファイルのビデオが再生されます。

最後のクラッシュの記録

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 作業ウィンドウの [トラブルシューティング（TroubleShooting）] タブをクリックします。

ステップ 3 [トラブルシューティング（Troubleshooting）] タブの [クラッシュの記録（Crash Recording）] 領域で、[記録の有効化（Enable Recording）] チェックボックスをオンにします。

注意 このタスクはトラブルシューティング目的のもので、常に有効にしていると Cisco IMC パフォーマンスに影響する場合があります。

ステップ 4 [変更の保存（Save Changes）] をクリックします。
[アクション（Actions）] 領域の [記録のキャプチャ（Capture Recording）] ボタンがイネーブルになります。

ステップ 5 （任意） [アクション（Actions）] 領域で、[記録のキャプチャ（Capture Recording）] をクリックし、自動的にクラッシュしたシステムの記録をキャプチャします。

（注） このオプションを選択すると、既存のクラッシュ レコードファイルが上書きされます。[OK] をクリックして、先へ進みます。

ステップ 6 サーバ上で実行された操作の記録を表示するには、[アクション（Actions）] 領域の [メッセージを再生する（Play Recording）] をクリックします。
サポートされている Java バージョンに関する手順を示した確認ダイアログ ボックスが表示されます。

ステップ 7 手順を確認し、[OK] をクリックします。
[DVR Player のコントロール（DVR Player Controls）] ダイアログボックスが表示されます。このダイアログボックスは、最後の数分にサーバ上で実行された操作の記録を再生します。この記録を確認して、システムがクラッシュした要因を分析できます。

ステップ 8 [クラッシュの記録（Crash Recording）] 領域の [アクション（Actions）] 領域で、[記録のダウンロード（Download Recording）] をクリックします。
ダウンロードするには、手順に従ってください。

（注） ファイルがローカル ドライブに `.dvc` 形式で保存されます。KVM プレーヤーまたはオフライン プレーヤーを使用してこの記録を表示できます。[記録のダウンロード（Download Recording）] オプションを選択するたびに、最後のクラッシュ プロセスが記録され、ファイル名が自動生成され、事前に指定されたパスに保存されます。

ステップ 9 ダウンロードが完了すると、記録のビデオを再生するファイルを選択できるので、選択して [開く（Open）] をクリックします。
[DVR Player のコントロール（DVR Player Controls）] ウィンドウが開き、選択したファイルのビデオが再生されます。

DVR Player のダウンロード

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [サーバ（Server）] タブをクリックします。

ステップ 2 [サーバ（Server）] タブの [トラブルシューティング（Troubleshooting）] をクリックします。

ステップ 3 [トラブルシューティング（Troubleshooting）] タブの [プレーヤー（Player）] 領域で、[プレーヤーのダウンロード（Download Player）] をクリックします。

ステップ 4 ダウンロードするには、手順に従ってください。これらのファイルは、ローカル ドライブに .tgz ファイル形式で zip 化されたファイルとして保存されます。
オフライン プレーヤーは、Windows、Linux、および MAC で保存されます。

ステップ 5 zip ファイルを解凍します。zip ファイルは通常、ブートストラップ ファイル下に保存され、名前は形式
`offline.tgz` に従います。

ステップ 6 ビデオ録画を確認するスクリプト ファイルを開きます。

（注） Windows で録画を再生する場合は、システムで起動している Java バージョンとスクリプト ファイル内のバージョンが同じであることを確認します。Windows のスクリプト ファイルが録画を再生しない場合は、次の手順に従います。

a) Windows のスクリプト ファイルをデスクトップに抽出します。
b) メモ帳を使用してファイルを開きます。
c) jre を検索し、システムで起動しているバージョンと一致するよう Java バージョンを置き換えます。デフォルトでは、Java のバージョンは jre7 に設定されています。
d) ファイルを保存します。
Java のバージョンを更新したら、抽出したファイルをデスクトップから削除できます。

（注） Java のバージョンの検証は Windows OS にのみ必要です。Linux および MAC の場合は、Java のバージョンが自動的に選択されます。

ステップ 7 スクリプト ファイルがダウンロードされるフォルダに移動し、ビデオ録画を再生するスクリプト ファイルを開きます。
DVR Player が開始され、サーバ上で実行された操作のビデオが再生されます。

KVM コンソールで DVR Player を使用した録画ビデオの再生

手順

ステップ 1 [ナビゲーション（Navigation）] ペインの [サーバ（Server）] タブをクリックします。

ステップ 2 [サーバ（Server）] タブの [センサー（Sensors）] をクリックします。

ステップ 3 [リモート プレゼンス（Remote Presence）] ペインの [仮想 KVM（Virtual KVM）] タブをクリックします。

ステップ 4 [仮想 KVM（Virtual KVM）] タブの [アクション（Actions）] 領域で、[KVM コンソールの起動（Launch KVM Console）] をクリックします。

（注） [作業（Work）]ペインの上部に表示されるツールバーの [KVM コンソールの起動（Launch KVM Console）] ボタンをクリックして KVM コンソールを開始することもできます。

[KVM コンソール（KVM Console）] が別ウィンドウで開きます。

ステップ 5 [KVM コンソール（KVM Console）] ウィンドウで、[ツール（Tools）] > [レコーダー/再生コントロール（Recorder /Playback Controls）] を選択します。

[DVR Player のコントロール（DVR Player Controls）] ウィンドウが開きます。

ステップ 6 [DVR Player のコントロール（DVR Player Controls）] ウィンドウで、[開く（Open）] ボタンをクリックします。

ステップ 7 記録を再生するファイルを選択し、[開く（Open）] をクリックします。
DVR Player が開始され、サーバ上で実行された操作のビデオが再生されます。

付 録 A

サーバ モデル別 BIOS パラメータ

ここでは、次の内容について説明します。

C220 M5 と C240 M5

I/O タブ

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

表 *16* : *[I/O]* タブの *BIOS* のパラメータ

[名前（Name）]	説明
[ホストを即座にリブート（Reboot Host Immediately）] チェックボックス	オンにすると、ホスト サーバが直ちに再起動されます。このチェックボックスは、変更を保存してからオンにする必要があります。
[レガシー USB サポート（Legacy USB Support）] ドロップダウン リスト	システムでレガシー USB デバイスをサポートするかどうか。次のいずれかになります。 • [無効（Disabled）] : USB デバイスは、EFI アプリケーションでのみ使用できます。 • [有効（Enabled）] : レガシー USB のサポートは常に使用できます。

[名前（Name）]	説明
[ダイレクト IO への Intel VT（Intel VT for directed IO）] ドロップダウン リスト	プロセッサで Intel Virtualization Technology（VT）を使用するかどうか。このテクノロジーでは、1 つのプラットフォームで、複数のオペレーティング システムとアプリケーションをそれぞれ独立したパーティション内で実行できます。次のいずれかになります。 • [無効（Disabled）]：プロセッサでの仮想化を禁止します。 • [有効（Enabled）]：プロセッサで、複数のオペレーティング システムをそれぞれ独立したパーティション内で実行できます。 （注） このオプションを変更した場合は、設定を有効にするためにサーバの電源を再投入する必要があります。
[Intel VTD coherency サポート（Intel VTD coherency support）] ドロップダウン リスト	プロセッサで Intel VT-d Coherency をサポートするかどうか。次のいずれかになります。 • [無効（Disabled）]：プロセッサでコヒーレンシをサポートしません。 • [有効（Enabled）]：プロセッサで VT-d Coherency を必要に応じて使用します。
[Intel VTD ATS サポート（Intel VTD ATS support）] ドロップダウン リスト	プロセッサで Intel VT-d Address Translation Services（ATS）をサポートするかどうか。次のいずれかになります。 • [無効（Disabled）]：プロセッサで ATS をサポートしません。 • [有効（Enabled）]：プロセッサで VT-d ATS を必要に応じて使用します。
[すべてのオンボード LOM Oprom（All Onboard LOM Oprom）] ドロップダウン リスト	オプション ROM がすべての LOM ポートで使用できるかどうか。次のいずれかになります。 • [無効（Disabled）]：すべてのポートでオプション ROM を無効にします。 • [有効（Enabled）]：すべてのポートでオプション ROM を有効にします。

[名前（Name）]	説明
[オンボード LOM ポート 0 Oprom（Onboard LOM Port0 Oprom）] ドロップダウン リスト	オプション ROM が LOM ポート 0 で使用できるかどうか。次のいずれかになります。 • [無効（Disabled）] : LOM ポート 0 でオプション ROM を使用できません。 • [有効（Enabled）] : LOM ポート 0 でオプション ROM を使用できます。
[オンボード LOM ポート 1 Oprom（Onboard LOM Port1 Oprom）] ドロップダウン リスト	オプション ROM が LOM ポート 1 で使用できるかどうか。次のいずれかになります。 • [無効（Disabled）] : LOM ポート 1 でオプション ROM を使用できません。 • [有効（Enabled）] : LOM ポート 1 でオプション ROM を使用できます。
[PCIe スロット *n* Oprom（Pcie Slot n Oprom）] ドロップダウン リスト	サーバが *n* で指定した PCIe カード スロットにあるオプション ROM を使用できるかどうか。次のいずれかになります。 • [無効（Disabled）] : スロット *n* のオプション ROM は使用できません。 • [有効（Enabled）] : スロット *n* のオプション ROM は使用可能です。
[MLOM Oprom] ドロップダウン リスト	このオプションでは、MLOM スロットに接続された PCIe アダプタのオプション ROM の実行を制御することができます。次のいずれかになります。 • [無効（Disabled）] : MLOM スロットに接続されている PCIe アダプタのオプション ROM を実行しません。 • [有効（Enabled）] : MLOM スロットに接続されている PCIe アダプタのオプション ROM を実行します。
[HBA Oprom] ドロップダウン リスト	このオプションでは、HBA スロットに接続された PCIe アダプタのオプション ROM の実行を制御することができます。次のいずれかになります。 • [無効（Disabled）] : HBA スロットに接続されている PCIe アダプタのオプション ROM を実行しません。 • [有効（Enabled）] : HBA スロットに接続されている PCIe アダプタのオプション ROM を実行します。

[名前（Name）]	説明
[フロントNVME1 Oprom（Front NVME1 Oprom）] ドロップダウン リスト	このオプションでは、SSD:NVMe1 スロットに接続された PCIe アダプタのオプションROMの実行を制御することができます。次のいずれかになります。 • [無効（Disabled）]：SSD:NVMe1 スロットに接続されている PCIe アダプタのオプション ROM を実行しません。 • [有効（Enabled）]：SSD:NVMe1 スロットに接続されている PCIe アダプタのオプション ROM を実行します
[フロントNVME2 Oprom（Front NVME2 Oprom）] ドロップダウン リスト	このオプションでは、SSD:NVMe2 スロットに接続された PCIe アダプタのオプションROMの実行を制御することができます。次のいずれかになります。 • [無効（Disabled）]：SSD:NVMe2 スロットに接続されている PCIe アダプタのオプション ROM を実行しません。 • [有効（Enabled）]：SSD:NVMe2 スロットに接続されている PCIe アダプタのオプション ROM を実行します
[HBA リンク速度（HBA Link Speed）] ドロップダウン リスト	このオプションを使用すると、PCIe HBA スロットに装着されているアダプタ カードの最大速度を制限できます。次のいずれかになります。 • [無効（Disabled）]：最大速度は制限されません。 • [自動（Auto）]：システムは許容最大速度を選択します。 • [GEN1]：最大2.5GT/s（ギガトランスファー/秒）までの速度が許可されます。 • [GEN2]：最大 5GT/s までの速度が許可されます。 • [GEN3]：最大 8GT/s までの速度が許可されます。
[MLOM リンク速度（MLOM Link Speed）] ドロップダウン リスト	このオプションを使用すると、PCIe MLOM スロットに装着されているアダプタ カードの最大速度を制限できます。次のいずれかになります。 • [無効（Disabled）]：最大速度は制限されません。 • [自動（Auto）]：システムは許容最大速度を選択します。 • [GEN1]：最大2.5GT/s（ギガトランスファー/秒）までの速度が許可されます。 • [GEN2]：最大 5GT/s までの速度が許可されます。 • [GEN3]：最大 8GT/s までの速度が許可されます。

[名前（Name）]	説明
[PCIe スロット *n* リンク速度（PCIe Slot n Link Speed）] ドロップダウン リスト	システム IO コントローラ *n*（SIOCn）アドオン スロット（*n* によって示される）のリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効であり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：リンク速度は第 2 世代まで到達可能です。 • [GEN3]：リンク速度は第 3 世代まで到達可能です。
[フロント NVME1 リンク速度（Front NVME1 Link Speed）] ドロップダウン リスト	NVMe フロント スロット 1 のリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効であり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：リンク速度は第 2 世代まで到達可能です。 • [GEN3]：リンク速度は第 3 世代まで到達可能です。
[フロント NVME2 リンク速度（Front NVME2 Link Speed）] ドロップダウン リスト	NVMe フロント スロット 2 のリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効であり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：リンク速度は第 2 世代まで到達可能です。 • [GEN3]：リンク速度は第 3 世代まで到達可能です。

[名前（Name）]	説明
[リア NVME1 リンク速度（Rear NVME1 Link Speed）] ドロップダウン リスト	NVMe 背面のスロット 1 のリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効であり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：リンク速度は第 2 世代まで到達可能です。 • [GEN3]：リンク速度は第 3 世代まで到達可能です。
[リア NVME2 リンク速度（Rear NVME2 Link Speed）] ドロップダウン リスト	NVMe 背面のスロット 2 のリンク速度。次のいずれかになります。 • [無効（Disabled）]：スロットは無効であり、カードは列挙されません。 • [自動（Auto）]：デフォルトのリンク速度。 リンク速度は自動的に割り当てられます。 • [GEN1]：リンク速度は第 1 世代まで到達可能です。 • [GEN2]：リンク速度は第 2 世代まで到達可能です。 • [GEN3]：リンク速度は第 3 世代まで到達可能です。
[VGA 優先順位（VGA Priority）] ドロップダウン リスト	システムに複数の VGA デバイスがある場合は、VGA グラフィックスデバイスのプライオリティを設定できます。次のいずれかになります。 • [オンボード（OnBoard）]：オンボード VGA デバイスが優先されます。BIOS ポスト画面および OS ブートはオンボード VGA ポート経由で駆動されます。 • [オフボード（OffBoard）]：PCIE グラフィックス アダプタが優先されます。BIOS ポスト画面および OS ブートは外部グラフィックス アダプタ ポート経由で駆動されます。 • [オンボードを無効（OnBoardDisabled）]：PCIE グラフィックス アダプタが優先され、オンボード VGA デバイスは無効になります。オンボード VGA が無効の場合、vKVM は機能しません。

[名前（Name）]	説明
[P-SATA OptionROM] ドロップダウン リスト	PCH SATA オプション ROM モードを選択できます。次のいずれかになります。 • [LSI SW Raid]：SATA コントローラと sSATA コントローラを LSI SW Raid の raid モードに設定します。 • [無効（Disabled）]：SATA コントローラと sSATA コントローラを無効にします。
[M2.SATA OptionROM] ドロップダウン リスト	Serial Advanced Technology Attachment（SATA）ソリッド ステート ドライブ（SSD）の動作モード。次のいずれかになります。 • [AHCI]： SATA コントローラと sSATA コントローラの両方を AHCI モードに設定します。 • [LSI SW Raid]：SATA コントローラと sSATA コントローラを LSI SW Raid の raid モードに設定します。 • [無効（Disabled）]：SATA コントローラと sSATA コントローラを無効にします。
[リア USB ポート（USB Port Rear）] ドロップダウン リスト	背面パネルの USB デバイスが有効か無効か。次のいずれかになります。 • [無効（Disabled）]：背面パネルの USB ポートを無効にします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されません。 • [有効（Enabled）]：背面パネルの USB ポートを有効にします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されます。
[フロント USB ポート（USB Port Front）] ドロップダウン リスト	前面パネルの USB デバイスが有効か無効か。次のいずれかになります。 • [無効（Disabled）]：前面パネルの USB ポートを無効にします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されません。 • [有効（Enabled）]：前面パネルの USB ポートを有効にします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されます。

[名前（Name）]	説明
[内部 USB ポート（USB Port Internal）] ドロップダウン リスト	内部USBデバイスが有効か無効か。次のいずれかになります。 • [無効（Disabled）]：内部の USB ポートを無効にします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されません。 • [有効（Enabled）]：内部の USB ポートを有効にします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されます。
[KVM USB ポート（USB Port KVM）] ドロップダウン リスト	KVM ポートが有効か無効か。次のいずれかになります。 • [無効（Disabled）]：KVM キーボードおよびマウス デバイスを無効にします。キーボードとマウスは KVM ウィンドウで機能しなくなります。 • [有効（Enabled）]：KVM キーボードおよびマウス デバイスを有効にします。
[SD カード USB ポート（USB Port SD Card）] ドロップダウン リスト	SD カードが有効か無効か。次のいずれかになります。 • [無効（Disabled）]：SD カードのポートを無効にします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されません。 • [有効（Enabled）]：SD カードのポートを有効にします。これらのポートに接続されるデバイスは、BIOS およびオペレーティング システムによって検出されます。
[IPV6 PXE サポート（IPV6 PXE Support）] ドロップダウン リスト	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。 • [無効（disabled）][無効（Disabled）]：IPV6PXE のサポートは利用できません。 • [有効（enabled）][有効（Enabled）]：IPV6PXE のサポートを常に利用できます。

サーバ管理タブ

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

表 *17* : *[サーバ管理（Server Management）] タブの BIOS パラメータ*

[名前（Name）]	説明
[ホストを即座にリブート（Reboot Host Immediately）] 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。
[OS ブート ウォッチドッグ タイマー ポリシー（OS Boot Watchdog Timer Policy）] ドロップダウン リスト	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。 • [電源オフ（Power Off）] : 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。 • [リセット（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、サーバはリセットされます。 （注） このオプションは [OS ブート ウォッチドッグ タイマー（OS Boot Watchdog Timer）] を有効にした場合にのみ適用されます。
[OS ウォッチドッグ タイマー（OS Watchdog Timer）] ドロップダウン リスト	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。 • [無効（Disabled）] : 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（Enabled）] : サーバ ブートにかかる時間をウォッチドッグ タイマーで追跡します。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 IMC 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。

[名前（Name）]	説明
[OS ブート ウォッチドッグ タイマー タイムアウト（OS Watchdog Timer Timeout）] ドロップダウン リスト	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。次のいずれかになります。 • [5 分（5 Minutes）] : OS ウォッチドッグ タイマーは、ブートが開始されてから 5 分後に期限が切れます。 • [10 分（10 Minutes）] : OS ウォッチドッグ タイマーは、ブートが開始されてから 5 分後に期限が切れます。 • [15 分（15 Minutes）] : OS ウォッチドッグ タイマーは、ブートが開始されてから 5 分後に期限が切れます。 • [20 分（20 Minutes）] : OS ウォッチドッグ タイマーは、ブートが開始されてから 5 分後に期限が切れます。 （注） このオプションは [OS ブート ウォッチドッグ タイマー（OS Boot Watchdog Timer）] を有効にした場合にのみ適用されます。

[名前（Name）]	説明
[ボー レート（Baud Rate）] ドロップダウン リスト	シリアル ポートの伝送速度として使用されるボー レート。[コンソール リダイレクション（Console Redirection）] を無効にした場合は、このオプションを使用できません。次のいずれかになります。 • [9.6k]：9,600 ボー レートが使用されます。 • [19.2k]：19,200 ボー レートが使用されます。 • [38.4k]：38,400 ボー レートが使用されます。 • [57.6k]：57,600 ボー レートが使用されます。 • [115.2k]：115,200 ボー レートが使用されます。 この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。
[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 リダイレクションに使用できるようにします。OS が起動した後は、コンソール リダイレクトは関係ありません。次のいずれかになります。 • [シリアル ポート A（Serial Port A）]：POST 中にシリアル ポート A でコンソール リダイレクションを有効にします。 • [シリアル ポート B（Serial Port B）]：POST 中にシリアル ポート B でコンソール リダイレクションを有効にします。 • [無効（Disabled）]：POST 中にコンソール リダイレクションは発生しません。

[名前（Name）]	説明
[CDN コントロール（CDN Control）] ドロップダウン リスト	イーサネット ネットワークの命名規則が Consistent Device Naming（CDN）または従来の命名規則に従うかどうか。次のいずれかになります。 • [無効（Disabled）]：VIC カードの CDN サポートが無効になります • [有効（Enabled）]：VIC カードの CDN サポートが有効になります。
[FRB 2 タイマー（FRB 2 Timer）] ドロップダウン リスト	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 Cisco IMC によって FRB2 タイマーが使用されるかどうか。次のいずれかになります。 • [無効（Disabled）]：FRB2 タイマーは使用されません。 • [有効（Enabled）]：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。
[フロー制御（Flow Control）] ドロップダウン リスト	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。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。 • [なし（None）]：フロー制御は使用されません。 • [RTS/CTS]：RTS/CTS がフロー制御に使用されます。 （注） この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。

[名前（Name）]	説明
[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。 • [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。

セキュリティ タブ

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

表 *18*：*[*セキュリティ（***Security***）*]* タブの ***BIOS*** パラメータ

[名前（**Name**）]	説明
[ホストを即座にリブート（**Reboot Host Immediately**）] 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。
[信頼されたプラットフォーム モジュールのサポート（Trusted Platform Module Support）] ドロップダウン リスト	信頼されたプラットフォーム モジュール（TPM）は、主に暗号キーを使用する基本的なセキュリティ関連機能を提供するように設計されたマイクロチップです。このオプションを使用すると、システムの TPM セキュリティ デバイス サポートを制御できます。次のいずれかを設定できます。 • [無効（Disabled）]：サーバは TPM を使用しません。 • [有効（Enabled）]：サーバは TPM を使用します。 （注） オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせください。
[電源オン パスワード（Power On Password）] ドロップダウン リスト	このトークンでは、F2 BIOS 設定を使用する前に BIOS パスワードを設定する必要があります。有効にすると、IO 設定、BIOS セットアップ、BIOS を使用したオペレーティング システムへの起動など、BIOS 機能にアクセスする前にパスワードを検証する必要があります。次のいずれかを設定できます。 • [無効（Disabled）]：サポートはディセーブルになっています。 • [有効（Enabled）]：サポートはイネーブルになっています。

[プロセッサ（Processor）] タブ

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

表 *19* : *[プロセッサ（Processor）] タブの BIOS パラメータ*

[名前（Name）]	説明
[Intel Virtualization Technology] ドロップダウン リスト	プロセッサで Intel Virtualization Technology（VT）を使用するかどうか。このテクノロジーでは、1 つのプラットフォームで、複数のオペレーティング システムとアプリケーションをそれぞれ独立したパーティション内で実行できます。次のいずれかになります。 • [無効（Disabled）] : プロセッサでの仮想化を禁止します。 • [有効（Enabled）] : プロセッサで、複数のオペレーティング システムをそれぞれ独立したパーティション内で実行できます。
[拡張 APIC（Extended APIC）] ドロップダウン リスト	拡張 APIC サポートを有効または無効にできます。次のいずれかになります。 • [有効（Enabled）] : APIC サポートを有効にします • [無効（Disabled）] : APIC サポートを無効にします。
[プロセッサ C1E（Processor C1E）] ドロップダウン リスト	C1 ステートに入ったときに、CPU が最小周波数に移行するかどうか。次のいずれかになります。 • [無効（Disabled）] : CPU は C1 ステートでも引き続き最大周波数で動作します。 • [有効（Enabled）] : CPU は最小周波数に移行します。このオプションでは C1 ステートで節約される電力量が最大になります。 （注） このオプションを使用できるのは一部の C シリーズ サーバだけです。

[名前（Name）]	説明
[プロセッサ C6 レポート（Processor C6 Report）] ドロップダウン リスト	BIOS からオペレーティング システムに C6 レポートを送信するかどうか。OS はレポートを受信すると、プロセッサを電力量の少ない C6 状態に移行してエネルギー使用量を減らし、最適なプロセッサ パフォーマンスを維持できます。次のいずれかになります。 • [無効（Disabled）] : BIOS から C6 レポートを送信しません。 • [有効（Enabled）] : BIOS から C6 レポートを送信し、OS がプロセッサを電力量の少ない C6 状態に移行できるようにします。 （注） [CPUPowerManagement] を [カスタム（Custom）] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。 （注） このオプションを使用できるのは一部の C シリーズ サーバだけです。
[XD ビット（Execute Disable Bit）] ドロップダウンリスト	アプリケーション コードを実行できる場所を指定するために、サーバのメモリ領域を分類します。この分類の結果、悪意のあるワームがバッファにコードを挿入しようとした場合、プロセッサでコードの実行を無効にします。この設定は、損害、ワームの増殖、および特定クラスの悪意のあるバッファ オーバーフロー攻撃を防止するのに役立ちます。次のいずれかになります。 • [無効（Disabled）] : プロセッサでメモリ領域を分類しません。 • [有効（Enabled）] : プロセッサでメモリ領域を分類します。 （注） オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせください。

[名前（Name）]	説明
[Intel Turbo Boost Tech] ドロップダウン リスト	プロセッサで Intel Turbo Boost Technology を使用するかどうか。Turbo Boost では、仕様よりも低い電力、温度、または電圧でプロセッサが動作していると、自動的にプロセッサの周波数が上がります。次のいずれかになります。 • [無効（Disabled）]：プロセッサの周波数は自動的には上がりません。 • [有効（Enabled）]：必要に応じてプロセッサで Turbo Boost Technology が利用されます。 （注） [CPUPowerManagement] を [カスタム（Custom）] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。
[Enhanced Intel SpeedStep Tech] ドロップダウン リスト	プロセッサで Enhanced Intel SpeedStep Technology を使用するかどうか。SpeedStep では、プロセッサの電圧やコア周波数をシステムが動的に調整します。SpeedStep を有効にすると、平均電力消費量と平均熱発生量が減少する可能性があります。次のいずれかになります。 • [無効（Disabled）]：プロセッサの電圧または周波数を動的に調整しません。 • [有効（Enabled）]：プロセッサで Enhanced Intel SpeedStep Technology が使用され、サポートされているすべてのスリープ状態でさらに電力を節約することが可能になります。 オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。 （注） [CPUPowerManagement] を [カスタム（Custom）] に設定する必要があります。そのようにしない場合、このパラメータの設定は無視されます。

[名前（Name）]	説明
[Intel HyperThreading Tech] ドロップダウンリスト	プロセッサで Intel Hyper-Threading Technology を使用するかどうか。Hyper-Threading 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。 • [無効（Disabled）] : プロセッサでのハイパースレッディングを禁止します。 • [有効（Enabled）] : プロセッサでの複数スレッドの並列実行を許可します。
[ワークロード設定（Workload Configuration）] ドロップダウン リスト	この機能を使用すると、ワークロードを最適化できます。オプションは[バランス（Balanced）] と [I/O に依存（I/O Sensitive）] です。 • NUMA • UMA
[コア マルチプロセッシング（Core MultiProcessing）] ドロップダウン リスト	サーバ上の 1 つ以上の物理コアを無効にできます。次のいずれかになります。 • [すべて（All）] : すべての物理コアを有効にします。 これにより、関連付けられている論理プロセッサ コアで Hyper Threading も有効になります。 • [1] ～ [28] : サーバで実行可能な論理プロセッサ コアの数を指定します。各物理コアには、論理コアが関連付けられています。 （注） オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせください。

[名前（Name）]	説明
[サブ NUMA クラスタリング（Sub NUMA Clustering）] ドロップダウンリスト	CPU がサブ NUMA クラスタリングをサポートするかどうか。そのクラスタリングでは、タグディレクトリとメモリ チャネルは常に同じ領域にあります。次のいずれかになります。 • [無効（disabled）][無効（Disabled）]：サブNUMAクラスタリングは発生しません。 • [有効（enabled）][有効（Enabled）]：サブ NUMA クラスタリングが発生します。 • [自動（Auto）][自動（auto）]：BIOS かサブNUMA のクラスタ リングされるかが決まります。
[IMC インターリーブ（IMC Interleave）] ドロップダウン リスト	この BIOS オプションは、Integrated Memory Controller（IMC）間のインターリーブを制御します。 • [一方向インターリーブ（1-way Interleave）]：インターリーブはありません。 • [双方向インターリーブ（2-way Interleave）]：2 つの IMC 間でアドレスがインターリーブされます。 • [自動（Auto）]：CPU が IMC のインターリーブ モードを決定します。
[XPT プリフェッチ（XPT Prefetch）] ドロップダウン リスト	XPTプリフェッチを使用して、最後のレベルのキャッシュに読み取り要求を送信できるようにして、その要求のコピーをメモリ コントローラのプリフェッチャに発行するかどうか。次のいずれかになります。 • [無効（disabled）][無効（Disabled）]：CPU は [XPT プリフェッチ（XPT Prefetch）] オプションを使用しません。 • [有効（enabled）][有効（Enabled）]：CPU は [XPT プリフェッチャ（XPT prefetcher）] オプションを有効にします。

[名前（Name）]	説明
[UPI プリフェッチ（UPI Prefetch）] ドロップダウン リスト	UPI プリフェッチは、DDR バス上でメモリ読み込みが早期に開始されるようにするメカニズムです。これは次のいずれかになります。 • [無効（disabled）][無効（Disabled）]：プロセッサでキャッシュデータをプリロードしません。 • [有効（enabled）][有効（Enabled）]：UPI プリフェッチャで最も関連性が高いと判断されたデータを含む L1 キャッシュをプリロードします。
[エネルギー パフォーマンスの BIOS 構成（Energy Performance BIOS Config）] ドロップダウン リスト	システムパフォーマンスまたはエネルギー効率がこのサーバで重要かどうかを判断できます。次のいずれかになります。 • [パフォーマンス（Performance）]：サーバでは、すべてのサーバ コンポーネントに全電力を常時提供します。このオプションでは、最高レベルのパフォーマンスが維持され、最大量の電力が必要となります。 • [バランス パフォーマンス（Balanced Performance）]：サーバは、すべてのサーバ コンポーネントに、パフォーマンスと電力のバランスを保つのに十分な電力を提供します。 • [バランス電力（Balanced Power）]：サーバは、すべてのサーバコンポーネントに、パフォーマンスと電力のバランスを保つのに十分な電力を提供します。 • [電力（Power）]：サーバは、すべてのサーバ コンポーネントに、消費電力の低減を維持するのに最大の電力を提供します。

[名前（Name）]	説明
[電力パフォーマンスの調整（Power Performance Tuning）] ドロップダウン リスト	BIOS または OS によってエネルギー パフォーマンスのバイアス調整をオンにできるかどうかを指定します。オプションは [BIOS] と [OS] です。 • [bios][BIOS]： エネルギー効率を調整する場合は [BIOS] を選択します。 • [os][OS]： エネルギー効率を調整する場合は [OS] を選択します。
[LLC プリフェッチ（LLC Prefetch）] ドロップダウン リスト	プロセッサが LLC プリフェッチ メカニズムを使用して日付を LLC にフェッチするかどうか。次のいずれかになります。 • [disabled][無効（Disabled）]：プロセッサでキャッシュデータをプリロードしません。 • [有効（enabled）][有効（Enabled）]：LLC プリフェッチャで最も関連性が高いと判断されたデータを含む L1 キャッシュをプリロードします。

[名前（Name）]	説明
[パッケージの C ステート（Package C State）]	アイドル時にサーバコンポーネントが使用できる電力量。次のいずれかになります。 • [no-limit][制限なし（No Limit）]：サーバは、使用可能な任意のCステートに入ることがあります。 • [自動（auto）][自動（Auto）]：物理的な高度をCPU が決定します。 • [C0 C1 ステート（C0 C1 State）]：サーバはすべてのサーバ コンポーネントに常にフル パワーを提供します。このオプションでは、最高レベルのパフォーマンスが維持され、最大量の電力が必要となります。 • [C2]：CPUのアイドル時に、システムの電力消費を C1 オプションよりもさらに低減します。この場合、必要な電力は C1 または C0 よりも少なくなりますが、サーバがハイ パフォーマンス モードに戻るのに要する時間が少し長くなります。 • [C6 保持なし（C6 Non Retention）]：CPU のアイドル時に、C3 オプションよりもさらに電力消費が低減されます。このオプションを使用すると、C0、C1、または C3 よりも電力量が節約されますが、サーバがフルパワーに戻るまでにパフォーマンス上の問題が発生する可能性があります。 • [C6 保持（C6 Retention）]：CPU のアイドル時に、C3 オプションよりもさらに電力消費が低減されます。このオプションを使用すると、C0、C1、または C3 よりも電力量が節約されますが、サーバがフルパワーに戻るまでにパフォーマンス上の問題が発生する可能性があります。

[名前（Name）]	説明
[ハードウェア P ステート（Hardware P-States）] ドロップダウン リスト	プロセッサハードウェアのPステートを有効にします。次のいずれかになります。 • [無効（disabled）][無効（Disabled）]：HWPMが無効になります。 • [hwpm-native-mode][HWPM ネイティブ モード（HWPM Native Mode）]：HWPMネイティブ モードがイネーブルになります。 • [hwpm-oob-mode][HWPM OOB モード（HWPM OOB Mode）]：HWPMアウトオブボックス モードがイネーブルになります。 • [レガシーなしのネイティブ モード（Native Mode with no Legacy）]（GUI のみ）

[メモリ（Memory）] タブ

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

表 *20*：*[メモリ（Memory）] タブの BIOS パラメータ*

名称	説明
[ホストを即座にリブート（Reboot Host Immediately）] チェックボックス	オンにすると、ホストサーバが直ちに再起動されます。このチェックボックスは、変更を保存してからオンにする必要があります。
[NUMA] ドロップダウン リスト	BIOS で Non-Uniform Memory Access（NUMA）がサポートされているかどうか。次のいずれかになります。 • [無効（Disabled）]：サポートはディセーブルになっています。 • [有効（Enabled）]：サポートはイネーブルになっています。

名称	説明
[メモリ RAS 構成の選択（Select Memory RAS configuration）] ドロップダウン リスト	サーバに対するメモリの信頼性、可用性、およびサービス性（RAS）の設定方法。次のいずれかになります。 • [最大パフォーマンス（Maximum Performance）]：システムのパフォーマンスが最適化されます。 • [ミラー モード 1LM（Mirror Mode 1LM）]：システムのメモリの半分をバックアップとして使用することにより、システムの信頼性が最適化されます。
[4 G 以上の復号化（Above 4G Decoding）] ドロップダウン リスト	4 GB 以上の MMIO を有効または無効にします。次のいずれかになります。 • [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。 （注） 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ります。

[電力/パフォーマンス（Power/Performance）] タブ

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

表 *21*：*[電力/パフォーマンス（Power/Performance）] タブの BIOS パラメータ*

[名前（Name）]	説明
[ホストを即座にリブート（Reboot Host Immediately）] チェックボックス	オンにすると、ホスト サーバが直ちに再起動されます。このチェックボックスは、変更を保存してからオンにする必要があります。

[名前（Name）]	説明
[ハードウェア プリフェッチャ（Hardware Prefetcher）] ドロップダウン リスト	プロセッサで、インテル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、統合2次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。 • [無効（Disabled）]：ハードウェア プリフェッチャは使用しません。 • [有効（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。
[隣接キャッシュ ライン プリフェッチャ（Adjacent Cache Line Prefetcher）] ドロップダウン リスト	プロセッサで必要な行のみを取得するのではなく、偶数または奇数のペアのキャッシュ行を取得するかどうか。次のいずれかになります。 • [無効（Disabled）]：プロセッサで必要な行のみを取得します。 • [有効（Enabled）]：プロセッサで必要な行およびペアの行の両方を取得します。
[DCU ストリーマ プリフェッチ（DCU Streamer Prefetch）] ドロップダウン リスト	プロセッサで DCU IP Prefetch メカニズムを使用して履歴キャッシュ アクセス パターンを分析し、L1 キャッシュ内で最も関連性の高い行をプリロードします。次のいずれかになります。 • [無効（Disabled）]：プロセッサはキャッシュ読み取り要求を予測しようとせず、明示的に要求された行のみを取得します。 • [有効（Enabled）]：DCU Prefetcher でキャッシュ読み取りパターンを分析し、必要と判断した場合にキャッシュ内の次の行を事前に取得します。
[DCU IP プリフェッチャ（DCU IP Prefetcher）] ドロップダウン リスト	プロセッサで DCU IP Prefetch メカニズムを使用して履歴キャッシュ アクセス パターンを分析し、L1 キャッシュ内で最も関連性の高い行をプリロードします。次のいずれかになります。 • [無効（Disabled）]：プロセッサでキャッシュ データをプリロードしません。 • [有効（Enabled）]：DCU IP Prefetcher で最も関連性が高いと判断されたデータを含む L1 キャッシュをプリロードします。

[名前（Name）]	説明
[CPU パフォーマンス（CPU Performance）] ドロップダウン リスト	上記のオプションに対し CPU パフォーマンス プロファイルを設定します。次のいずれかになります。 • [エンタープライズ（Enterprise）]：すべてのオプションが有効です。 • [HPC]：すべてのオプションが有効です。 この設定はハイパフォーマンス コンピューティングとも呼ばれます。 • [高スループット（Hight Throughput）]：DCU IP プリフェッチャのみが有効になります。残りのオプションは無効になります。 • [カスタム（Custom）]：パフォーマンス プロファイルのすべてのオプションをサーバの BIOS セットアップから設定できます。また、[ハードウェア プリフェッチャ（Hardware Prefetcher）] オプションと [隣接キャッシュ ライン プリフェッチャ（Adjacent Cache Line Prefetcher）] オプションも同様に設定できます。

索 引

記号

B

C

F

G

H

I

J

K

L

N

O

P

S

T

U

V

W

X

あ

い

え

お

く

こ

さ

し

す

せ

た

つ

て

と

な

ね

は

ふ

ほ

ま

め

ゆ

り

る

ろ