Cisco UCS C シリーズ サーバ Integrated Management Controller リリース 3.0 GUI コンフィギュレーション ガイド（C22 M3、C24 M3、C220 M3、および C240 M3 サーバ用）

初版：2016 年 12 月 13 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**で示しています。 CLI コマンド内の変数は、イタリック体（*italic*）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

Cisco UCS の関連ドキュメント

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、http://www.cisco.com/go/unifiedcomputing/b-series-doc で入手可能な『*Cisco UCS B-Series Servers Documentation Roadmap*』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 C22 M3 ラックマウント サーバ
- Cisco UCS C24 M3 ラックマウント サーバ
- Cisco UCS C220 M3 ラックマウント サーバ
- Cisco UCS C240 M3 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 を使ってサーバに OS をインストールするために、Cisco IMCを使用できます。

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 IMCCLI を呼び出すために Cisco IMC GUI を使用する。
- Cisco IMCCLI で呼び出したコマンドを Cisco IMC GUI に表示する。
- Cisco IMCGUI 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を使用すると次のサーバ管理タスクを実行できます。

- サーバの電源オン、電源オフ、電源の再投入、リセット、およびシャットダウン
- ロケータ LED の切り替え
- BIOS の設定

- サーバのブート順の設定
- サーバのプロパティとセンサーの表示
- リモート プレゼンスの管理
- ローカル ユーザ アカウントの作成と管理、および Active Directory によるリモート ユーザ認証の有効化
- 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
- HTTP、SSH、IPMI Over LAN、SNMP などのコミュニケーション サービスの設定
- 証明書の管理
- プラットフォーム イベント フィルタの設定
- Cisco IMCファームウェアの更新
- 障害、アラーム、およびサーバのステータスのモニタリング
- タイム ゾーンの設定およびローカル タイムの表示
- Cisco IMCファームウェアのインストールおよび有効化
- BIOS ファームウェアのインストールおよび有効化

オペレーティング システムまたはアプリケーションのプロビジョニングおよび管理はできない

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

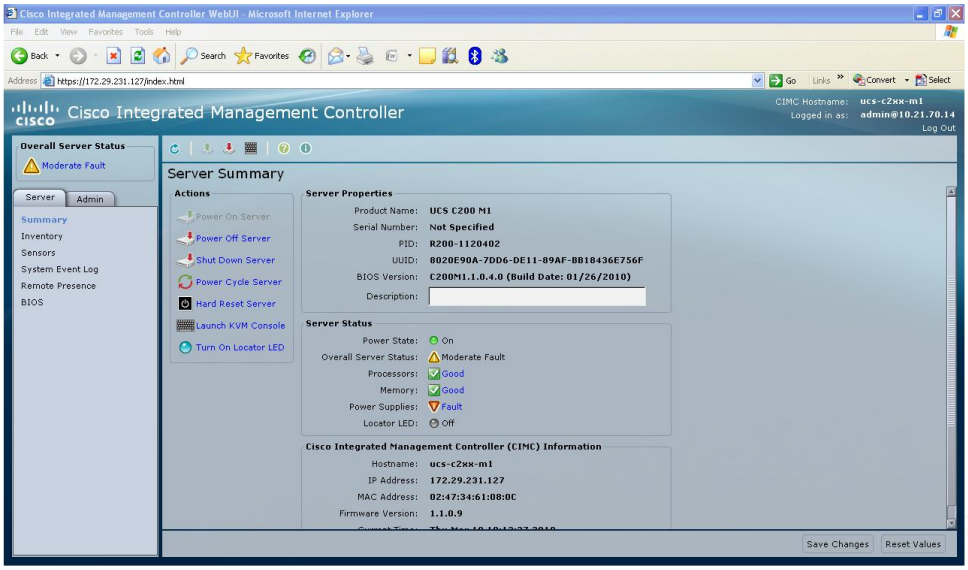
Cisco IMCユーザ インターフェイスは、Cisco C シリーズ サーバの Web ベースの管理インターフェイスです。Cisco IMCユーザ インターフェイスを起動して、次の最小要件を満たしているすべてのリモート ホストからサーバを管理できます。

- Sun JRE 1.8.0_ 45 ～ Sun JRE 1.8.0_ 60
- 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が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 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、ユーザ インターフェイスが次の図のように表示されます。



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

[ナビゲーション（Navigation）]ペインは、Cisco IMC GUI の左側に表示されます。[ナビゲーション（Navigation）]ペインの [サーバ（Server）]、[管理者（Admin）]、または[ストレージ（Storage）] タブにあるリンクをクリックすると、関連付けられたタブが右側の [ワーク（Work）] ペインに表示されます。

[ナビゲーション（Navigation）]ペインには次の領域があります。

- [全体のサーバ ステータス（Overall Server Status）]領域
- [サーバ（Server）]タブ
- [管理者（Admin）]タブ
- [ストレージ（Storage）]タブ

[全体のサーバ ステータス（Overall Server Status）]領域

[全体のサーバステータス（OverallServer Status）] 領域は、[サーバ（Server）]、[管理者（Admin）]、および[ストレージ（Storage）]タブの上にあります。[ワーク（Work）]ペインの [サーバ サマリー（Server Summary）] タブをリフレッシュするには、領域内のリンクをクリックします。

（注） 別のタブが [ワーク（Work）]ペインに表示される場合は、このリンクをクリックすると、更新されたサーバ情報で [サーバ サマリー（Server Summary）] タブが再表示されます。

[サーバ（Server）]タブ

[サーバ（Server）]タブの各ノードは、[ワーク（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。

[サーバ（Server）]タブのノード名	[ワーク（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、ステータス、BIOS のバージョン、Cisco IMCファームウェアのバージョン、IP アドレス、および MAC アドレス。
インベントリ	インストール済みの CPU、メモリ カード、電源、PCIアダプタ、Cisco VIC アダプタ、ネットワーク アダプタ、ストレージ アダプタ、TPM、SAS エクスパンダ、PID カタログ。
[センサー（Sensors）]	電源、ファン、温度、電圧、電流、LED、およびストレージ センサーの読み取り。
リモート プレゼンス（Remote Presence）	KVM、仮想メディア、および Serial over LAN の設定。

[サーバ（Server）]タブのノード名	[ワーク（Work）]ペインのタブで提供される情報
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。
電源ポリシー（Power Policies）	電源ポリシーの設定。
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。
トラブルシューティング	ブートストラッププロセスの記録、クラッシュ記録、およびプレーヤー。

[管理者（Admin）]タブ

[管理者（Admin）]タブの各ノードは、[ワーク（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）]タブのノード名	[ワーク（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。
ネットワーク	NIC、IPv4、VLAN、および 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	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。
イベント管理	プラットフォーム イベント フィルタ。
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	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。

[ストレージ（Storage）]タブ

[ストレージ（Storage）]タブの各ノードは、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 Cisco FlexFlash コントローラに対応します。

各ノードは、[ワーク（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）]タブのノード名	[ワーク（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）	選択された MegaRAID コントローラまたは Cisco Flexible Flash コントローラに関する一般情報。
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。

ツールバー

ツールバーは [ワーク（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。
サーバの電源オン（Power On Server）	サーバの電源を投入します。
サーバの電源オフ（Power Off Server）	サーバの電源を切ります。
[KVM コンソール起動（Launch KVM Console）]	KVM コンソールを起動します。
ping	[Ping 詳細（Ping Details）]ペインを起動します。
ヘルプ	[ワーク（Work）]ペインに表示されるタブのオンライン ヘルプを表示します。
情報（Info）	Cisco IMC情報を表示します。

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 IMCCisco 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 IMCCisco 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

はじめる前に

Adobe Flash Player 10 以降がインストールされていない場合は、ローカル マシンにインストールします。

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 IMCWeb 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 ウィンドウを閉じる、またはキャンセルすることはできません。タブを開いたり、ブラウザページを更新したりしても、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、初期設定にリセットした後か、1.5(x) または 2.0(1) バージョンから最新バージョンに Cisco IMCをアップグレードした後のログイン時に表示されます。
- 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。ただし、これに伴うリスクは完全に個人の責任となります。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の右上にある [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 OS を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 [サーバ（Server）] タブをクリックします。

ステップ 4 [サーバ（Server）] タブの [リモート プレゼンス（Remote Presence）] をクリックします。

ステップ 5 [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 6 [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。

[KVM コンソール（KVM Console）]が別ウィンドウで開きます。

ステップ 7 KVM コンソールから、[VM]タブをクリックします。

ステップ 8 [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 9 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。
サーバをリブートすると、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

サーバの管理

この章の内容は、次のとおりです。

全体のサーバ 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 [全体のサーバ ステータス（Overall Server Status）] 領域で、青色のヘルス レポート リンクをクリックして、[サーバ サマリー（Server Summary）] ペインを更新します。

ステップ 2 （任意） [サーバ サマリー（Server Summary）]ペインの [サーバのステータス（Server Status）] 領域で次の情報を確認します。

（注） 次に、表示される可能性のあるすべてのステータス フィールドを示します。実際に表示されるフィールドは、使用しているCシリーズサーバのタイプによって異なります。

[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）] • [重大な障害（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
[プロセッサ（Processors）] フィールド	プロセッサの全体的なステータス。次のいずれかになります。 • Good • Fault このフィールドのリンクをクリックして、プロセッサに関する詳細情報を表示できます。 （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。
[DIMM の全体のステータス（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。
[電源装置（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。

[名前（Name）]	説明
[HDD]フィールド	ハードドライブの全体的なステータス。次のいずれかになります。 • Good • 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。 （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。
[ロケータ LED（Locator LED）]フィールド	ロケータ LED がオンかオフか。
[前面ロケータ 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。
[ストレージの全体のステータス（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）

サーバ使用率の表示

一部の UCS C シリーズ サーバでのみサーバ使用率を確認できます。

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 [サマリー（Summary）] をクリックします。

ステップ 3 [サーバ サマリー（Server Summary）]ペインの [サーバ使用率（Server Utilization）] 領域で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。

（注） これらの使用率の値は、ハードウェアの合計帯域幅のパーセンテージとして報告されます。これらの値は、ホスト ベースのリソース モニタリング ソフトウェアで表示される値と一致しないことがあります。

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 [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 [サマリー（Summary）] をクリックします。

ステップ 3 [アクション（Actions）]領域で、[ロケータ LED をオンにする（Turn On Locator LED）] をクリックします。
[ロケータ LED（Locator LED）]フィールドの LED インジケータが点灯し、サーバの物理ロケータ LED がオンになって点滅します。

ステップ 4 [アクション（Actions）]領域で、[ロケータ LED をオフにする（Turn Off Locator LED）] をクリックします。
ロケータ LED がオフになります。

シャーシの前面ロケータ LED の切り替え

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

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 [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 [サマリー（Summary）] をクリックします。

ステップ 3 [アクション（Actions）]領域で、[前面ロケータ LED をオンにする（Turn On Front Locator LED）] ボタンをクリックします。
[ロケータ LED（Locator LED）] フィールドの LED インジケータが点灯し、シャーシの物理ロケータ LED がオンになって点滅します。

ステップ 4 [アクション（Actions）]領域で、[前面ロケータ LED をオフにする（Turn Off Front Locator LED）] をクリックします。
前面ロケータ LED がオフになります。

ハード ドライブのロケータ LED の切り替え

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

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 [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 [センサー（Sensors）]ペインの [ストレージ（Storage）] タブをクリックします。

ステップ 4 [ストレージ（Storage）]テーブルで、ロケータ LED を変更するハードディスク ドライブ（HDD）を見つけます。

ステップ 5 その HDD の [LED ステータス（LED Status）]カラムで、ドロップダウン リストから目的のロケータ LED の状態を選択します。

[オンにする（Turn On）]を選択すると、このカラムの LED ステータス インジケータが点灯し、関連付けられた HDD の物理ロケータ LED がオンになって点滅します。

タイム ゾーンの選択

タイム ゾーンの選択

タイム ゾーンの選択により、ローカル タイム ゾーンを選択できるため、デフォルトのマシンの時刻ではなく、ローカル タイムを表示できます。Cisco IMCWeb UI および CLI では、希望するタイム ゾーンを選択して設定するオプションが提供されます。

タイムゾーンをローカルタイムに設定すると、システムのタイミングを使用するすべてのサービスにタイム ゾーンの変数が適用されます。これは、ロギング情報に影響し、Cisco IMCの次のアプリケーションで利用されます。

- 障害サマリーと障害履歴のログ
- Cisco IMCのログ
- rsyslog

ローカル タイムを設定すると、表示できるアプリケーションのタイムスタンプが、選択したローカル タイムで更新されます。

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 [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 [サマリー（Summary）] をクリックします。

ステップ 3 [Cisco Integrated Management Controller（Cisco IMC）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。

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 [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 [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。

サーバのブート順の管理

Server Boot Order

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可能ですが、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設定され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 [実際のブート順序（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 [実際のブート順序（Actual Boot Order）]領域に [ポリシー ターゲットなし（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、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 [設定済みブート順序（Configured Boot Order）]領域でこれらのデバイスを確認できます。CLI でこれらのデバイスを確認するには、**show boot-device** コマンドを入力します。この間に、サーバ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、[実際のブート順序（Actual Boot Order）]領域でこれを確認できます。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はレガシー 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。

Configuring the Precision Boot Order

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 [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[BIOS] をクリックします。
[BIOS] ページが表示されます。

ステップ 3 [アクション（Actions）]領域で、[ブート順序の設定（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 この説明を確認してから、[OK]をクリックします。
[ブート順序の設定（Configure Boot Order）]ダイアログボックスが表示されます。

ステップ 5 [ブート順序の設定（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。

[名前（Name）]	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） • PCHStorage の追加（Add PCHStorage） • UEFISHELL の追加（Add UEFISHELL）
[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	選択したブート可能デバイスを [ブート順序（Boot Order）]テーブルから削除します。
[クローン（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）]テーブルで優先順位の高い位置に移動します。
[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）]テーブルで優先順位の低い位置に移動します。

[名前（Name）]	説明
[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、そのサーバが次に再起動するときに、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	変更の保存または既存の設定の再適用を行わずに、ダイアログボックスを閉じます。 このオプションを選択すると、そのサーバが次に再起動するときに、実際のブート順は変更されません。

ステップ 6 [保存（Save）]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 [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[BIOS] をクリックします。

ステップ 3 [アクション（Action）]領域の [ブート順序の設定（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 この説明を確認してから、[OK]をクリックします。

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

ステップ 5 [ブート順序の設定（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。

[名前（Name）]	**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。範囲は次のように C シリーズ サーバによって異なります。 • C220 M4 および C240 M4 サーバの場合は、「HBA」を入力します。 • C460 M4 サーバの場合は、1 ～ 255 の範囲の値、または「SAS」を入力します。 • 他の C シリーズ サーバの場合は、1 ～ 255 の範囲の値、または「M」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）。
[スロット（Slot）]フィールド	• C220 M4 および C240 M4 サーバの場合は、1 ～ 255 の値か「L」または「MLOM」を入力します。 • C3160 サーバの場合は、1 ～ 255 の値を入力します。 • C460M4 サーバの場合は、1 ～ 255 の値か「L1」または「L2」を入力します。 • 他の C シリーズ サーバの場合は、0 ～ 255 の値または「L」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。
[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。

SAN ブート デバイスを追加するには、[SAN の追加（Add SAN）]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
[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。範囲は次のように C シリーズ サーバによって異なります。 • C220 M4 および C240 M4 サーバの場合は、1 ～ 255 の値、または「MLOM」を入力します。 • C460M4 サーバの場合は、1 ～ 255 の値か「L1」または「L2」を入力します。 • 他の C シリーズ サーバの場合は、1 ～ 255 の値を入力します。
[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。
[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。

iSCSI ブートデバイスを追加するには、[iSCSI の追加（Add iSCSI）]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
[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。範囲は次のように C シリーズ サーバによって異なります。 • C220 M4 および C240 M4 サーバの場合は、1 ～ 255 の値か「L」または「MLOM」を入力します。 • C3160 サーバの場合は、1 ～ 255 の値を入力します。 • C460M4 サーバの場合は、1 ～ 255 の値か「L1」または「L2」を入力します。 • 他の C シリーズ サーバの場合は、1 ～ 255 の値または「L」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。
[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。

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）。
[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。

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。
[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。

[名前（Name）]	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）。
[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。

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）
[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）。
[追加（Add）]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。

[名前（Name）]	説明
[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）。
[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。
[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 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ように、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：POST センサー、システム ファームウェア エラー。EFI ロード イメージ セキュリティ違反。[0x5302] がアサートされました。（System Software event: Post sensor, System Firmware error. EFI Load Image Security Violation. [0x5302] was asserted.）

UEFI のセキュア ブートは次のコンポーネントでサポートされます。

コンポーネント	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
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	

コンポーネント	タイプ
LSI	• LSI MegaRAID SAS 9240-8i • LSI MegaRAID SAS 9220-8i • LSI MegaRAID SAS 9265CV-8i • LSI MegaRAID SAS 9285CV-8e • LSI MegaRAID SAS 9285CV-8e • LSI MegaRAID SAS 9266-8i • LSI SAS2008-8i mezz • LSI Nytro カード

UEFI セキュア ブートのイネーブル化

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの [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[BIOS] 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 オプションをディセーブルにしないと、[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 [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[BIOS] 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 [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[BIOS] をクリックします。
[BIOS]ページが表示されます。

ステップ 3 [BIOS]ページの [実際のブート順序（Actual Boot Order）] 領域で、サーバが最後にブートされたときに BIOS が実際に使用した順序で表示されるブート デバイスのリストを確認します。
最後のブート時に存在するすべてのデバイスが線形順に示されます。デバイスのストリング名を展開し、その特定のデバイスの属性を確認できます。

（注） BIOS は、設定されているブート順の設定に一致しないデバイスを検出し、それらを [ポリシー ターゲットなし（NonPolicyTarget）] デバイスとしてデバイス リストに表示します。

ワンタイム ブート デバイスでブートするサーバの設定

現在設定されているブート順を中断せずに、次回のサーバ起動時のみ、特定のデバイスからサーバが起動するように設定できます。サーバがワンタイムブートデバイスから起動した後は、以前に設定したブート順で以降のすべてのリブートが行われます。

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[BIOS] をクリックします。

ステップ 3 [BIOS プロパティ（BIOS Properties）]領域で、[ワンタイム ブート デバイスの設定（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） 無効な高度ブート デバイスで設定されていても、ホストはワンタイム ブート デバイスに対して起動されます。

サーバのリセット

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 [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 [サマリー（Summary）] をクリックします。

ステップ 3 [アクション（Actions）]領域で、[サーバのハードリセット（Hard Reset Server）] をクリックします。

「サーバをハードリセットしますか?（HardReset the Server?）」というメッセージがダイアログボックスに表示されます。

ステップ 4 [OK]をクリックします。

サーバのシャットダウン

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 [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 [サマリー（Summary）] をクリックします。

ステップ 3 [アクション（Actions）]領域で、[サーバのシャットダウン（Shut Down Server）] をクリックします。
「サーバをシャットダウンしますか?（ShutDown the Server?）」というメッセージがダイアログボックスに表示されます。

ステップ 4 [OK]をクリックします。

サーバの電源管理

サーバの電源投入

（注） サーバの電源がCisco IMC経由以外の何らかの方法でオフにされた場合、サーバは電源をオンにしてもすぐにはアクティブになりません。サーバは、Cisco IMCが初期化を完了するまでスタンバイ モードで動作します。

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 [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 [サマリー（Summary）] をクリックします。

ステップ 3 [アクション（Actions）]領域で、[サーバの電源オン（Power On Server）] をクリックします。
「サーバの電源をオンにしますか?（Poweron the server?）」というメッセージがダイアログボックスに表示されます。

ステップ 4 [OK]をクリックします。

サーバの電源オフ

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 [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 [サマリー（Summary）] をクリックします。

ステップ 3 [アクション（Actions）]領域で、[サーバの電源オフ（Power Off Server）] をクリックします。
「シャーシ ファームウェアのアップデートが使用可能です。続行しますか?（Thereis an update available for Chassis Firmware, would you like to continue?）」というメッセージがダイアログボックスに表示されます。[OK]をクリックすると、サーバの電源が切れ、システム ファームウェアが更新されます。

ステップ 4 [OK]をクリックします。

サーバ電源の再投入

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 [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 [サマリー（Summary）] をクリックします。

ステップ 3 [アクション（Actions）]領域で、[サーバの電源の再投入（Power Cycle Server）] をクリックします。
「サーバの電源を再投入しますか?（PowerCycle the Server?）」というメッセージがダイアログボックスに表示されます。

ステップ 4 [OK]をクリックします。

電力ポリシーの設定

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 [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 [電源ポリシー（Power Policies）] をクリックします。

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 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 5 [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（PowerOff）]：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（PowerOn）]：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。 • [前回の状態の復元（RestoreLast 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。

[名前（Name）]	説明
[電力遅延タイプ（Power Delay Type）]ドロップダウン リスト	選択されたポリシーが [電源オン（PowerOn）] の場合、このオプションを使用して再起動を遅らせることができます。次のいずれかになります。 • [固定（fixed）]：サーバは一定の遅延後に再起動します。 • [ランダム（random）]：サーバはランダムな遅延後に再起動します。 （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。
[電力遅延値（Power Delay Value）]フィールド	固定遅延が選択されている場合、シャーシの電源が復元されてCisco IMCの再起動が完了したら、システムはサーバを再起動する前に、指定された秒数だけ待機します。 0 ～ 240 の整数を入力します。 （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。

ステップ 6 [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

ファン制御ポリシー

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

- 最大の CPU パフォーマンス

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

- 低電力消費

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

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

次のファン ポリシーの中から選択できます。

- バランス

  これがデフォルトのポリシーです。この設定でほとんどのサーバ構成を冷却できますが、容易に加熱する PCIe カードを含むサーバには適さない可能性があります。

- 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。この設定では、[バランス（Balanced）] ファン ポリシーと同じ速度またはそれより高速でファンが作動します。

- 低電力（Low Power）

  この設定は、PCIe カードが含まれない最小構成のサーバに最適です。

- 高電力（High Power）

  この設定は、60 ～ 85 % の範囲の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 プラットフォームごとに異なりますが、およそ 60 ～ 85 % の範囲内です。

- 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プラットフォームごとに異なりますが、およそ 70 ～ 100 % の範囲内です。

（注） Cisco IMCでファン ポリシーを設定することはできますが、実際のファン作動速度はサーバの構成要件により決定されます。たとえば、ファン ポリシーを [バランス（Balanced）]に設定しても、容易に加熱するPCIeカードがサーバに含まれる場合は、過熱を防ぐためにサーバのファン速度が必要な最小のファン速度に自動的に調整されます。ファン速度を必要以上に高く設定している場合、システムは選択されたファン速度を保持します。[適用済みのファン ポリシー（Applied Fan Policy）]には、サーバで実行されている実際のファン速度が表示されます。

[設定ステータス（Configuration Status）]には、設定されたファン ポリシーのステータスが表示されます。次のいずれかになります。

- [成功（SUCCESS）] : 選択されたファン ポリシーはサーバで実行されている実際のファン速度に一致します。
- [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の可能性があります。
  - 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 ポリシーのオーバーライド（FAN POLICY OVERRIDE）] : 指定されたファン速度を、サーバの構成要件によって決定された実際の速度で上書きします。

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 [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 [電源ポリシー（Power Policies）] 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）]：デフォルトのポリシーです。この設定でほとんどのサーバ構成を冷却できますが、容易に過熱する PCIe カードを含むサーバには適さ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。この設定では、[バランス（Balanced）]ファン ポリシーで設定された速度と同じ速度またはより高速でファンが作動します。 • [低電力（LowPower）]：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（HighPower）]：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 % の範囲内です。 • [最大電力（MaximumPower）]：この設定は、70 ～ 100 % の範囲の非常に高速な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 % の範囲内です。
[適用済みのファン 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。 設定したファン 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。

[名前（Name）]	説明

[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の可能性があります。
	  • 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 ポリシーのオーバーライド（FAN POLICY OVERRIDE）] : 指定されたファン速度を、サーバの構成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。

PID カタログの概要

現在、スタンドアロン ラック サーバ上の製品 ID（PID）カタログは、新しい Cisco IMC イメージまたは新しいコンテナでのみ更新されます。これは、新しいデバイスがサーバに追加されても、新しい Cisco IMC イメージが生成されるまで PID カタログが古い状態のままであることを意味します。

このリリースでは、PID カタログのみを個別に更新できます。Cisco IMC またはコンテナを更新する必要はありません。FTP、TFTP、SFTP、HTTP、および SCP を使用して、署名付きの PID 更新パッケージをダウンロードできます。ダウンロード後は、署名付きの PID 更新パッケージが検証され、新しい「pid-update-catalog.xml」が生成されます。**show* - pid** コマンドを使用すると、既存の catalog.xml がこの XML ファイルに置き換えられます。

PID カタログの更新は次の手順で構成されます。

- PID 更新パッケージの作成
- パッケージのセキュリティ確保と署名
- カタログの一般的更新の保護

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 [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 [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）]ペインで [PID カタログ（PID Catalog）] タブをクリックします。

ステップ 4 [アクション（Actions）]領域で [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 5 [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の選択（Choose File to Upload）] ダイアログボックスを使用してアップロード対象のカタログ 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表示されます。

ステップ 6 [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

[名前（Name）]	説明
[サーバIP/ホスト名（Server IP/Hostname）]フィールド	PID カタログ情報を使用できるサーバの 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。
[アップロード（Upload）]ボタン	選択した PID カタログをアップロードします。 （注） リモート サーバ タイプとして SCP または SFTP を選択してこのアクションを実行した場合、ポップアップ ウィンドウに「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 カタログのアクティブ化

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。
- PID カタログの [アップロード ステータス（Upload Status）] が [はい（Yes）] と表示される必要があります。

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの [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 [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）]ペインで [PID カタログ（PID Catalog）] タブをクリックします。

ステップ 4 [アクション（Actions）]領域で [PID カタログのアクティブ化（Activate PID Catalog）] リンクをクリックします。
確認用のダイアログボックスが表示されます。[はい（Yes）] を選択して PID カタログをアクティブ化するか、[いいえ（No）] を選択してアクティベーションをキャンセルします。

（注） 初めてシステムにログオンしたときは、[PID カタログのアクティブ化（Activate PID Catalog）]リンクが無効になっています。このリンクは PID カタログをサーバにアップロードしないと有効になりません。

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。

シナリオ	動作
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。

- 空の FlexFlash をサーバに追加し、SD ファームウェアを旧バージョンから最新バージョンにアップグレードします。

  この作業を完了する方法については、を参照してください。

- 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 IMCGUI 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 IMCGUI 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。

`Flexible Flash コントローラと通信できません：操作 ffCardsGet、ステータス CY_AS_ERROR_INVALID_RESPONSE（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 IMCCLI 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 *1*：*C220*、*C240*、*C22*、*C24*、*C460 M4* の運用プロファイルのフィールド

[名前（Name）]	説明
[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。
[有効な仮想ドライブ（Virtual Drives Enabled）]フィールド	USB形式のドライブとして、サーバに対して使用可能にできる仮想ドライブ。 単一 HV パーティションに対するチェックボックスが表示されます。 （注） 旧バージョンでは、各仮想ドライブに対して 4 個のチェックボックスが表示されます。単一パーティションをすでに作成し、旧バージョンの Cisco IMCにダウングレードしている場合、HV のみが有効であっても他の仮想ドライブが表示されます。
[RAID プライマリ メンバ（RAID Primary Member）] フィールド	プライマリ RAID メンバが存在するスロット。
[RAID セカンダリ ロール（RAID Secondary Role）] フィールド	値は secondary-active にする必要があります。

[名前（Name）]	説明
[I/O 読み取りエラーしきい値（I/O Read Error Threshold）] フィールド	Cisco Flexible Flash カードへのアクセス時に許可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。
[I/O 書き込みエラーしきい値（I/O Write Error Threshold）] フィールド	Cisco Flexible Flash カードへのアクセス時に許可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。
[エラーのクリア（Clear Errors）]チェックボックス	オンにした場合、[変更の保存（Save Changes）]をクリックすると、読み取り/書き込みエラーがクリアされます。

（注）
- 次の表は、C220 M4 および C240 M4 サーバでのみ有効です。
- [ミラー（Mirror）]モードでは、[スロット 1 の読み取り/書き込みエラーしきい値（Slot1 Read/Write Error Threshold）] が両方の SD カード（カードが 2 枚ある場合）に適用されます。
- [Util]モードでは、[スロット 1 の読み取り/書き込みエラーしきい値（Slot1 Read/Write Error Threshold）] がスロット 1 のカードに適用され、[スロット 2 の読み取り/書き込みエラーしきい値（Slot2 Read/Write Error Threshold）] がスロット 2 のカードに適用されます。

表 *2*：*C220 M4*、*C240 M4* の運用プロファイルのフィールド

[名前（Name）]	説明
[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。
[ファームウェアの動作モード（Firmware Operating Mode）] フィールド	現在のファームウェアの動作モード。次のいずれかになります。 • ミラー（Mirror） • Util

[名前（Name）]	説明
[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 へのアクセス時に許可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。
[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 へのアクセス時に許可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。
[スロット 2 読み取りエラーしきい値（SLOT-2 Read Error Threshold）]フィールド	Cisco Flexible Flash カードのスロット 2 へのアクセス時に許可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。
[スロット 2 書き込みエラーしきい値（SLOT-2 Write Error Threshold）]フィールド	Cisco Flexible Flash カードのスロット 2 へのアクセス時に許可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 [変更の保存（Save Changes）]をクリックします。

Flexible Flash コントローラ ファームウェア モードの設定

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、[ファームウェア モードの設定（Configure Firmware Mode）] をクリックします。

ステップ 4 確認ボックスで [OK]をクリックします。
コントローラ ファームウェア モードを現在のファームウェア モードから他のモードに切り替えます。

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。

[名前（Name）]	説明
[ミラー（Mirror）]オプションボタン	カードを RAID 1 ミラー構成に設定するには、このオプションを選択します。カードをミラーモードに設定した場合の影響は次のとおりです。 • 選択されたスロットのカードは、ミラープライマリ正常としてマークされます。 • もう一方のスロットのカードは、ミラーセカンダリ非正常としてマークされます。 • 1 つの RAID パーティションが作成されます。同期が完了するまで、RAID ステータスは低下状態になります。 • カードの読み取り/書き込みエラー数および読み取り/書き込みしきい値は 0 に設定されます。 • ホストの接続が停止される可能性があります。 次を入力します。 • [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：オンにすると、選択したプライマリ カード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、[物理ドライバ情報（Physical Driver Info）] 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

[名前（Name）]	説明
[Util]オプション ボタン	カードを[Util]モードに設定するには、このオプションを選択します。カードを Util モードに設定した場合の影響は次のとおりです。 • 選択したスロット内のカードで 4 つのパーティションが作成されます。各パーティションはそれぞれ SCU、HUU、ドライバのユーティリティ用と、ユーザが使用できるパーティションで、カードは正常とマークされます。 • 他のスロット内のカード（ある場合）では、単一パーティションが作成され、そのカードは正常とマークされます。 • カードの読み取り/書き込みエラー数および読み取り/書き込みしきい値は 0 に設定されます。 • ホストの接続が停止される可能性があります。 • 設定されたカードはペアになります。 次を入力します。 • [ユーザ パーティション名（User Partition Name）]フィールド：Util カードの 4 番目のパーティションに割り当てる名前。 • [非 Util カードのパーティション名（Non Util Card Partition Name）]フィールド：2 枚目のカードがある場合、その単一パーティションに割り当てる名前。 • [Util カードの選択（Select Util Card）]ドロップダウン：Util 用に設定するスロット。次のいずれかになります。 ◦ [Slot1] ◦ [Slot2] ◦ [なし（None）]：サーバにSD カードが 1 枚ある場合にのみ適用されます。

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 カードからのブート

Cisco Flexible Flashカード上のブート可能な仮想ドライブを指定し、サーバに定義されているデフォルトのブート順に関係なく、サーバが次に再起動されたときにデフォルトのブート優先順位を上書きすることができます。指定したブート デバイスは一度だけ使用されます。サーバがリブートした後、この設定は無効になります。Cisco Flexible Flashカードが使用可能な場合にのみ、ブート可能な仮想ドライブを選択できます。それ以外の場合は、サーバはデフォルトのブート順を使用します。

（注） サーバをリブートする前に、選択する仮想ドライブがCisco Flexible Flashカード上でイネーブルになっていることを確認してください。[ストレージ（Storage）]タブに移動してカードを選択し、[仮想ドライブ情報（Virtual Drive Info）] サブタブに進みます。

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 [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[BIOS] をクリックします。

ステップ 3 [アクション（Actions）]領域で、[ブート オーバーライド優先順位の設定（Configure Boot Override Priority）] をクリックします。
[ブート オーバーライド優先順位（Boot Override Priority）]ダイアログボックスが表示されます。

ステップ 4 [ブート オーバーライド優先順位（Boot Override Priority）]ドロップダウン リストから、ブートに使用する仮想ドライブを選択します。

ステップ 5 [Apply]をクリックします。

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。

ISO イメージ設定の追加

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 Util モードで設定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 [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、イメージを追加する仮想ドライブを選択し、[イメージの追加（Add Image）] をクリックします。

ステップ 5 [イメージの追加（Add 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。次のいずれかになります。 • SCU • 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]：CommonInternet File System。
[リモート共有（Remote Share）]フィールド	マッピングするイメージの 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。
[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

[名前（Name）]	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。オプションは選択した [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
[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	選択したユーザ名のパスワード（必要な場合）。

ステップ 6 [保存（Save）]をクリックします。

ISO 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。
- 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。

- このタスクは、カードが [Util]モードで設定されている場合にのみ使用できます。

（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 [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、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。

（注） SCU および HUU の更新には最大 1 時間、ドライバの更新には最大 5 時間かかる場合があります。

ISO イメージのマップ解除

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。
- 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 [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、イメージのマッピングを解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。

Cisco Flexible Flashカード設定のリセット

Cisco Flexible Flashカードのスロットの設定をリセットした場合の影響は次のとおりです。

- 選択されたスロットのカードは、プライマリ正常としてマークされます。
- もう一方のスロットのカードは、セカンダリ アクティブ非正常としてマークされます。
- 1 つの RAID パーティションが作成されます。
- カードの読み取り/書き込みエラー数および読み取り/書き込みしきい値は0に設定されます。
- ホストの接続が停止される可能性があります。

最新バージョンにアップグレードして、設定のリセット オプションを選択した場合、単一ハイパーバイザ（HV）パーティションが作成され、既存の4パーティション設定は消去されます。これにより、データ損失が生じることもあります。失われたデータを取り出すことができるのは、HVパーティションにまだデータを書き込んでおらず、以前のバージョンにダウングレードする場合だけです。

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 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、[パーティション デフォルトのリセット（Reset Partition Defaults）] をクリックします。

ステップ 4 [パーティション デフォルトのリセット（Reset Partition Defaults）]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
[スロット（Slot）]オプションボタン	カードをプライマリ正常としてマークするスロットを選択します。 他のスロットにカードがある場合は、セカンダリ アクティブ非正常としてマークされます。
[パーティション デフォルトのリセット（Reset Partition Defaults）]ボタン	選択したスロットの設定をリセットします。
[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 5 [はい（Yes）]をクリックします。

Cisco Flexible Flash カードの設定の保持

次の状況では、ファームウェア バージョン 253 以降のカードをサポートする FlexFlash の設定を保持できます。

- 2 つの非ペアの FlexFlash があります。
- 単一 FlexFlash からサーバが稼働していて、非ペアの FlexFlash が他のスロットにあります。
- 1 つの FlexFlash がファームウェア バージョン 253 をサポートし、もう 1 つの FlexFlash はパーティション化されていません。

設定を保持した場合の影響は次のとおりです。

- 選択されたスロットの FlexFlash の設定は、もう 1 つのカードにコピーされます。
- 選択されたスロットのカードは、プライマリ正常としてマークされます。
- セカンダリ スロットのカードは、セカンダリ アクティブ非正常としてマークされます。

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 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 [カード設定の同期（Synchronize Card Configuration）] をクリックします。

ステップ 4 [カード設定の同期（Synchronize Card Configuration）]ダイアログボックスで、次のフィールドを更新します。

[名前（Name）]	説明
[スロット（Slot）]オプションボタン	設定を保持するスロットを選択します。選択したスロットから他のスロットのカードに設定がコピーされ、選択したスロットのカードはプライマリ正常としてマークされます。
[カード設定の同期（Synchronize Card Configuration）]ボタン	選択したカードのタイプが SD253 で単一の HV 設定が存在する場合にのみ、選択したカードから設定をコピーします。
[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 5 [はい（Yes）]をクリックします。

SD カードの追加およびファームウェア 1.5(4) バージョンへのアップグレード

手順

ステップ 1 サーバのスロット 2 に空の SD カードを挿入します。

ステップ 2 Cisco IMC ソフトウェアのバージョンをリリース 1.5(4) にアップグレードして、Cisco IMC をリブートします。

ステップ 3 [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 4 タブの [Cisco FlexFlash] をクリックします。

ステップ 5 [コントローラ情報（Controller Info）]タブで、[内部状態（Internal State）] フィールドに表示されている状態を確認します。
状態は [WAIT_ON_USER]と表示されている必要があります。

ステップ 6 [FlexFlash コントローラのリセット（Reset FlexFlash Controller）]をクリックします。

重要 このオプションにより、ホストへのパーティションの列挙がリセットされます。FlexFlash コントローラをリセットする前に、SD カードがホストから使用されていないことを確認してください。

FlexFlash コントローラをリセットすると、スロット 1 のカードは自動的にプライマリ正常としてマークされ、スロット 2 の空のカードはセカンダリ アクティブ非正常カードとしてマークされます。RAID 正常性は [低下（Degraded）] と表示されます。この状況では、すべてのデータ トランザクションが正常カードに書き込まれ、データのミラーリングは行われません。

ステップ 7 （任意） RAID 正常性を「正常」に変更するには、ホスト上で Cisco UCS Server Configuration Utility（Cisco UCS SCU）を起動して [ハイパーバイザ同期（Hypervisor Sync）]をクリックします。

このオプションにより、正常なカードから非正常カードにデータがミラーリングされます。

Cisco IMCおよび SD カードのファームウェア バージョンのアップグレード

SD ストレージは、単一 HV パーティション設定としてCisco IMCバージョン 1.5(4) で利用でき、ファームウェア バージョン 257 をサポートします。以前のリリースでは、4 パーティション設定があり、ファームウェア バージョン 247、248、および 253 がサポートされていました。Cisco IMC バージョン 1.5(4) は、257 より前のすべての SD カードのファームウェア バージョンをサポートします。ファームウェア バージョン 253 以降の SD カードの場合は、[FlexFlash コントローラのリセット（Reset FlexFlash Controller）]オプションを選択すると、これらのカードのファームウェア バージョンが 257 に自動的にアップグレードされます。

Cisco IMC バージョン 1.4(x) から 1.5(4) へのアップグレード

リリース 1.4(x) のパーティション レイアウトは、リリース 1.5(4) とは著しく異なるので、Cisco IMCバージョン 1.4(x) から 1.5(4) への自動アップグレードは不可能です。Cisco IMCバージョン 1.4(x) を 1.5(4) に直接アップグレードすると、[パーティション デフォルトのリセット（Reset Partition Default）]オプションを選択するよう求めるプロンプトが表示されます。このオプションを選択すると、単一 HV パーティション設定が作成されます。これは、SD カードに保管されたデータの損失をもたらす場合があります。4 パーティション設定と SD カードに保存されたデータを保持するために、まずCisco IMCバージョンを 1.5(2) または 1.5(3) にアップグレードし、その後 1.5(4) バージョンにアップグレードすることを推奨します。[FlexFlash コントローラのリセット（Reset FlexFlash Controller）]オプションを選択します。

Cisco IMC、SD カード ファームウェアのアップグレード、および新しい SD カードの追加

はじめる前に

- RAID1 ミラーを正常に作成するには、追加される空のカードのサイズが、既存のカードのサイズと一致する必要があります。
- 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 SD 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。特定の SD カードを正常としてマークするには、[パーティションデフォルトのリセット（Reset Partition Defaults）]をクリックします。その結果として、もう 1 つのカードがセカンダリ アクティブ非正常カードとしてマークされます。

手順

ステップ 1 Cisco IMC ソフトウェアのバージョンをリリース 1.5(4) にアップグレードして、Cisco IMC をリブートします。

ステップ 2 [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 3 タブの [Cisco FlexFlash] をクリックします。

ステップ 4 [コントローラ情報（Controller Info）]タブで、[内部状態（Internal State）] フィールドに表示されている状態を確認します。
状態は [WAIT_ON_USER]と表示されている必要があります。

ステップ 5 [FlexFlash コントローラのリセット（Reset FlexFlash Controller）]をクリックします。

重要 このオプションにより、ホストへのパーティションの列挙がリセットされます。FlexFlash コントローラをリセットする前に、SD カードがホストから使用されていないことを確認してください。

FlexFlash コントローラをリセットすると、スロット 1 のカードは自動的にプライマリ正常としてマークされ、スロット 2 の空のカードはセカンダリ アクティブ非正常カードとしてマークされます。RAID 正常性は [低下（Degraded）]と表示されます。この状況では、すべてのデータ トランザクションが正常カードに書き込まれ、データのミラーリングは行われません。

ステップ 6 タブの [Cisco FlexFlash] をクリックします。

ステップ 7 [コントローラ情報（Controller Info）]タブで [パーティションデフォルトのリセット（Reset Partition Defaults）] をクリックし、プライマリ スロットとして [スロット 1（SLOT-1）] を選択します。
スロット 1 のカードが自動的にプライマリ正常としてマークされ、スロット 2 の空のカードがセカンダリ アクティブ非正常カードとしてマークされます。RAID 正常性は [低下（Degraded）] と表示されます

ステップ 8 （任意） RAID 正常性を「正常」に変更するには、ホスト上で Cisco UCS Server Configuration Utility（Cisco UCS SCU）を起動して [ハイパーバイザ同期（Hypervisor Sync）]をクリックします。

このオプションにより、正常なカードから非正常カードにデータがミラーリングされます。

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 で 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 エラーが検出された場合、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、修正可能なエラー 16000 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 のブラックリスト化の有効化

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 [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 [メモリ（Memory）]ペインの [DIMM ブラック リスト（DIMM Black Listing）] 領域で、[DIMM ブラック リストを有効にする（Enable DIMM Black List）] チェックボックスをオンにします。

Configuring BIOS Settings

主要な BIOS 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 [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[BIOS] をクリックします。

ステップ 3 [アクション（Actions）] 領域で[BIOS の設定（Configure BIOS）] をクリックします。

ステップ 4 ダイアログ ボックス で、[メイン（Main）] タブをクリックします。

ステップ 5 変更を保存した後にサーバをリブートするかどうかを指定します。
[変更を保存（Save Changes）] をクリックした後で変更内容を自動的に適用するには、[ホストを即座にリブート（Reboot Host Immediately）]チェックボックスをオンにします。Cisco IMCによってサーバがただちにリブートされて、変更が適用されます。

変更内容を後で適用するには、[ホストを即座にリブート（Reboot Host Immediately）]チェックボックスをオフにします。Cisco IMCによって変更が保存され、次回サーバがリブートするときに適用されます。

（注） 保留中の BIOS パラメータの変更がすでにある場合、Cisco IMCは、[変更を保存（Save Changes）] をクリックしたときに、保存されている値を現在の設定で自動的に上書きします。

ステップ 6 [メイン（Main）]タブで、BIOS 設定のフィールドを更新します。
使用可能な BIOS パラメータは、使用しているサーバのモデルによって異なります。各 BIOS 設定のオプションに関する説明および情報については、次を参照してください。

- サーバ モデル別 BIOS パラメータ，（347 ページ）

ステップ 7 （任意） [BIOS パラメータの設定（Configure BIOS Parameters）]ダイアログ ボックスの下部にあるボタンを使用して、パラメータのリセットまたはデフォルト値の復元を行うことができます。
次のオプションを使用できます。

[名前（Name）]	説明
[変更を保存（Save Changes）] ボタン	3 つのタブすべての BIOS パラメータの設定を保存し、ダイアログボックスを閉じます。 [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。
[値のリセット（Reset Values）] ボタン	3 つのタブすべての BIOS パラメータの値を、このダイアログボックスが最初に開いたときに有効であった設定に戻します。
[デフォルトの復元（Restore Defaults）] ボタン	3 つのタブすべての BIOS パラメータをそれぞれのデフォルト設定に設定します。
[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。

重要 このダイアログボックスのボタンは、現在表示しているタブのパラメータだけでなく、使用可能なすべてのタブのすべての BIOS パラメータに影響します。

ステップ 8 [変更の保存（Save Changes）]をクリックします。

高度な BIOS の設定

（注） 搭載されているハードウェアによっては、このトピックで説明されている一部の設定オプションが表示されない場合があります。

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 [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[BIOS] をクリックします。

ステップ 3 [アクション（Actions）] 領域で[BIOS の設定（Configure BIOS）] をクリックします。

ステップ 4 ダイアログ ボックス で、[高度（Advanced）] タブをクリックします。

ステップ 5 変更を保存した後にサーバをリブートするかどうかを指定します。

[変更を保存（Save Changes）] をクリックした後で変更内容を自動的に適用するには、[ホストを即座にリブート（Reboot Host Immediately）]チェックボックスをオンにします。Cisco IMCによってサーバがただちにリブートされて、変更が適用されます。

変更内容を後で適用するには、[ホストを即座にリブート（Reboot Host Immediately）]チェックボックスをオフにします。Cisco IMCによって変更が保存され、次回サーバがリブートするときに適用されます。

（注） 保留中の BIOS パラメータの変更がすでにある場合、Cisco IMCは、[変更を保存（Save Changes）] をクリックしたときに、保存されている値を現在の設定で自動的に上書きします。

ステップ 6 [高度（Advanced）]タブで、BIOS 設定のフィールドを更新します。
使用可能な BIOS パラメータは、使用しているサーバのモデルによって異なります。各 BIOS 設定のオプションに関する説明および情報については、次を参照してください。

- サーバ モデル別 BIOS パラメータ，（347 ページ）

ステップ 7 （任意） [BIOS パラメータの設定（Configure BIOS Parameters）]ダイアログ ボックスの下部にあるボタンを使用して、パラメータのリセットまたはデフォルト値の復元を行うことができます。次のオプションを使用できます。

[名前（Name）]	説明
[変更を保存（Save Changes）] ボタン	3 つのタブすべての BIOS パラメータの設定を保存し、ダイアログボックスを閉じます。 [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。
[値のリセット（Reset Values）] ボタン	3 つのタブすべての BIOS パラメータの値を、このダイアログボックスが最初に開いたときに有効であった設定に戻します。
[デフォルトの復元（Restore Defaults）] ボタン	3 つのタブすべての BIOS パラメータをそれぞれのデフォルト設定に設定します。
[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。

重要 このダイアログボックスのボタンは、現在表示しているタブのパラメータだけでなく、使用可能なすべてのタブのすべての BIOS パラメータに影響します。

ステップ 8 [変更の保存（Save Changes）]をクリックします。

サーバ管理 BIOS 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 [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[BIOS] をクリックします。

ステップ 3 [アクション（Actions）] 領域で[BIOS の設定（Configure BIOS）] をクリックします。

ステップ 4 ダイアログ ボックス で、[サーバ管理（Server Management）] タブをクリックします。

ステップ 5 変更を保存した後にサーバをリブートするかどうかを指定します。
[変更を保存（Save Changes）] をクリックした後で変更内容を自動的に適用するには、[ホストを即座にリブート（Reboot Host Immediately）]チェックボックスをオンにします。Cisco IMCによってサーバがただちにリブートされて、変更が適用されます。

変更内容を後で適用するには、[ホストを即座にリブート（Reboot Host Immediately）]チェックボックスをオフにします。Cisco IMCによって変更が保存され、次回サーバがリブートするときに適用されます。

（注） 保留中の BIOS パラメータの変更がすでにある場合、Cisco IMCは、[変更を保存（Save Changes）] をクリックしたときに、保存されている値を現在の設定で自動的に上書きします。

ステップ 6 [サーバ管理（Server Management）]タブで、BIOS 設定のフィールドを更新します。
使用可能な BIOS パラメータは、使用しているサーバのモデルによって異なります。各 BIOS 設定のオプションに関する説明および情報については、次を参照してください。

- サーバ モデル別 BIOS パラメータ, （347 ページ）

ステップ 7 （任意） [BIOS パラメータの設定（Configure BIOS Parameters）]ダイアログ ボックスの下部にあるボタンを使用して、パラメータのリセットまたはデフォルト値の復元を行うことができます。
次のオプションを使用できます。

[名前（Name）]	説明
[変更を保存（Save Changes）] ボタン	3 つのタブすべての BIOS パラメータの設定を保存し、ダイアログボックスを閉じます。 [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。

[名前（Name）]	説明
[値のリセット（Reset Values）] ボタン	3 つのタブすべての BIOS パラメータの値を、このダイアログボックスが最初に開いたときに有効であった設定に戻します。
[デフォルトの復元（Restore Defaults）] ボタン	3 つのタブすべての BIOS パラメータをそれぞれのデフォルト設定に設定します。
[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。

重要 このダイアログボックスのボタンは、現在表示しているタブのパラメータだけでなく、使用可能なすべてのタブのすべての BIOS パラメータに影響します。

ステップ 8 [変更の保存（Save Changes）]をクリックします。

BIOS セットアップの開始

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。
- 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 [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[BIOS] をクリックします。

ステップ 3 [アクション（Actions）]領域で [BIOS セットアップの開始（Enter BIOS Setup）] をクリックします。

ステップ 4 [有効（Enable）]をクリックします。
BIOS セットアップの開始が有効になります。再起動すると、サーバは BIOS セットアップを開始します。

BIOS の工場出荷時のデフォルト設定への復元

BIOS のコンポーネントが目的のとおりに動作しなくなる状況では、カスタマイズされた製造時のデフォルト値に BIOS セット アップ トークンおよびパラメータを復元できます。

（注） このアクションは、一部の C シリーズ サーバに対してのみ使用できます。

はじめる前に

- サーバの電源をオフ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 [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[BIOS] をクリックします。

ステップ 3 [アクション（Actions）]領域で、[工場出荷時のデフォルト設定への復元（Restore Manufacturing Custom Defaults）] をクリックします。

ステップ 4 [OK]をクリックします。

BIOS プロファイル

Cisco UCS Server では、すべてのサーバ プラットフォームにデフォルトのトークン ファイルを使用できます。また、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。サーバの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、トークン値が正しい組み合わせで事前設定されたトークン ファイルを利用できます。使用可能な事前設定済みプロファイルには、仮想化、高パフォーマンス、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各種トークン ファイルをダウンロードし、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することができます。これにより、ターンアラウンド タイムをかけずに要件に合わせてプロファイルをカスタマイズすることが可能です。

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 クライアント経由で 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 [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[BIOS] をクリックします。

ステップ 3 [アクション（Actions）]領域で [BIOS プロファイルの設定（Configure BIOS Profile）] 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 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 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使用できるサーバの 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	選択した BIOS プロファイルをアップロードします。 （注） リモート サーバ タイプとして SCP または SFTP を選択してこのアクションを実行した場合、ポップアップ ウィンドウに「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表示されます。

次の作業

BIOS プロファイルをアクティブ化します。

BIOS プロファイルのアクティブ化

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 [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[BIOS] をクリックします。
[BIOS] ページが表示されます。

ステップ 3 [アクション（Actions）]領域で [BIOS プロファイルの設定（Configure BIOS Profile）] をクリックします。

ステップ 4 [BIOS プロファイル（BIOS プロファイル）]領域で [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化します。

次の作業

既存の BIOS プロファイルを削除します。

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 [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[BIOS] をクリックします。
[BIOS] ページが表示されます。

ステップ 3 [アクション（Actions）]領域で [BIOS プロファイルの設定（Configure BIOS Profile）] をクリックします。

ステップ 4 [BIOS プロファイル（BIOS Profile）]領域で [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 [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[BIOS] をクリックします。
[BIOS] ページが表示されます。

ステップ 3 [アクション（Actions）]領域で [BIOS プロファイルの設定（Configure BIOS Profile）] をクリックします。

ステップ 4 [BIOS プロファイル（BIOS プロファイル）]領域で [バックアップの作成（Take Backup）] 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 プロファイルのバックアップを作成します。

次の作業

BIOS プロファイルをアクティブ化します。

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 [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[BIOS] をクリックします。
[BIOS] ページが表示されます。

ステップ 3 [アクション（Actions）]領域で [BIOS プロファイルの設定（Configure BIOS Profile）] をクリックします。

ステップ 4 [BIOS プロファイル（BIOS Profile）]領域で [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	アップロードしたファイルに指定された値が表示されます。
[実際の値（Actual Value）]カラム	アクティブな BIOS 設定の値が表示されます。

第 4 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。

サーバ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 [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 [サマリー（Summary）] をクリックします。

ステップ 3 [サーバ サマリー（Server Summary）]ペインの [サーバのプロパティ（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。

[名前（Name）]	説明
[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。
[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。

Cisco IMC情報の表示

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 [サマリー（Summary）] をクリックします。

ステップ 3 [サーバ サマリー（Server Summary）]ペインの [Cisco Integrated Management Controller（CIMC）情報（Cisco Integrated Management Controller (CIMC) Information）][Cisco Integrated Management Controller（Cisco IMC）情報（Cisco Integrated Management Controller (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。

[名前（Name）]	説明
[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、BIOS および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。
[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。

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 [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 [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。

[名前（Name）]	説明
[ベンダー（Vendor）]フィールド	CPU のベンダー。
[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）。
[バージョン（Version）]フィールド	CPU のバージョン。
[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 [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 [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。

[名前（Name）]	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）。
[障害が発生したメモリ（Failed Memory）]フィールド	現在障害が発生しているメモリの量（MB 単位）。

[名前（Name）]	説明
[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。
[無視されたメモリ（Ignored Memory）]フィールド	現在使用できないメモリの量（MB 単位）。
[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。
[無視された 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。
[利用可能なメモリ 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（MaximumPerformance）]：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。

[名前（Name）]	説明
[DIMM の全体のステータス（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。 • [正常（Good）]：DIMMステータスは使用可能です。 • [重大な障害（Severe Fault）]：修正不可能なECC エラーが発生している場合の DIMM ステータス。
[DIMM ブラック リストを有効にする（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。

[名前（Name）]	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）。
[メモリ タイプ（Memory 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。

[名前（Name）]	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]：MicronTechnology, Inc. • [0x5105]：QimondaAG i. In. • [0x802C]：MicronTechnology, Inc. • [0x80AD]：HynixSemiconductor Inc. • [0x80CE]：SamsungElectronics, Inc. • [0x8551]：QimondaAG i. In. • [0xAD00]：HynixSemiconductor Inc. • [0xCE00]：SamsungElectronics, 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）。
[部品番号（Part Number）]カラム	ベンダーによって割り当てられた DIMM の部品番号。
[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）。

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 [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 [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 [電源（Power Supplies）] タブをクリックします。

ステップ 4 各電源で次の情報を確認します。

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。

[名前（**Name**）]	説明
[デバイス ID（Device ID）]カラム	電源装置ユニットの ID。
[入力（Input）]カラム	電源装置への入力（ワット単位）。 （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。
[最大出力（Max Output）]カラム	電源装置からの最大出力（ワット単位）。 （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。
[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装置の製品識別子。

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 [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 [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）]カラム	アダプタの名前。
[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たセカンダリ 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たセカンダリ デバイス ID。

Nvidia GPU カード情報の表示

この情報は、すべての Cisco UCS C シリーズ サーバで使用できるわけではありません。

はじめる前に

使用可能な Nvidia GPU カードの情報を表示するには、サーバの電源が入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 [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 [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）]カラム	アダプタの名前。
[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たセカンダリ 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たセカンダリ デバイス ID。

ステップ 5 [スロット ID（Slot ID）]または Nvidia GPU カードの [製品名（Product Name）] をクリックします。

ステップ 6 [GPU インベントリ（GPU Inventory）]ダイアログボックスで、Nvidia GPU カードに関する次の情報を確認します。

[名前（Name）]	説明
GPU ID	NVidia カードの GPU の ID。
温度	GPU カードの温度（摂氏単位）。

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 [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 [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（Equipped）] : TPM はホストサーバに存在します。 • [空（Empty）] : TPMはホスト サーバに存在しません。
[モデル（Model）]カラム	TPM のモデル番号。TPM がホスト サーバに存在しない場合、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がホスト サーバに存在しません。
[ベンダー（Vendor）]カラム	TPMベンダーの名前。TPMがホストサーバに存在しない場合、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がホスト サーバに存在しません。 （注） TPM バージョン 2.0 がインストールされた一部の C シリーズ サーバでは、[アクティブ ステータス（Active Status）]に [適用しない（NA）] と表示されます。
[シリアル（Serial）]カラム	TPM のシリアル番号。TPM がホスト サーバに存在しない場合、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。 • [未所有（Unowned）] : TPMは所有されていません。 • [不明（Unknown）] : TPMがホスト サーバに存在しません。 （注） TPM バージョン 2.0 がインストールされた一部の C シリーズ サーバでは、[所有（Ownership）]ステータスに [適用しない（NA）] と表示されます。
[リビジョン（Revision）]カラム	TPM のリビジョン番号。TPM がホスト サーバに存在しない場合、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 [管理者（Admin）] タブをクリックします。

ステップ 2 [サーバ（Server）] タブの [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）]ペインで [PID カタログ（PID Catalog）] タブをクリックします。

ステップ 4 [アクション（Actions）]領域で、

ステップ 5 [サマリー（Summary）]領域で、PID カタログに関する次のサマリー情報を確認します。

[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） • ダウンロード成功（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：ダウンロードに失敗しました（Download Error - Download Failed） • アクティベーション成功（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 6 [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 7 [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 8 [PCI アダプタ（PCI Adapter）]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たセカンダリ アダプタ ID。

[名前（Name）]	説明
[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たセカンダリ デバイス ID。

ステップ 9 [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 5 章

センサーの表示

この章の内容は、次のとおりです。

電源センサーの表示

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。

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　[センサー（Sensors）]ペインの [電源（Power Supply）] タブをクリックします。

ステップ 4　[プロパティ（Properties）]領域で、[冗長性ステータス（Redundancy Status）]フィールドにサーバの電源装置の冗長性のステータスが表示されます。

ステップ 5　[個別センサー（Discrete Sensors）]領域で、サーバに関する次の統計情報を確認できます。

[名前（Name）]	説明
[センサー名（Sensor Name）] カラム	センサーの名前。
[ステータス（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） • Non-Recoverable
[リーディング（Reading）] カラム	センサーの基本状態。

ステップ 6 [しきい値センサー（Threshold Sensors）]領域で、サーバに関する次の統計情報を確認できます。

[名前（Name）]	説明
[センサー名（Sensor Name）] カラム	センサーの名前。
[ステータス（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） • 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）。
[Warning 最小しきい値（Warning Threshold Min）] カラム	Warning の最小しきい値。

[名前（Name）]	説明
[Warning 最大しきい値（Warning Threshold Max）] カラム	Warning の最大しきい値。
[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。

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 [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 [センサー（Sensors）]ペインの [ファン（Fan）] タブをクリックします。

ステップ 4 サーバのファンに関する次の統計情報が表示されます。

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。

[名前（Name）]	説明
[センサー名（Sensor Name）] カラム	センサーの名前。
[ステータス（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） • Non-Recoverable

[名前（Name）]	説明
[速度（Speed）]カラム	ファンの速度（RPM 単位）。
[Warning 最小しきい値（Warning Threshold Min）] カラム	Warning の最小しきい値。
[Warning 最大しきい値（Warning Threshold Max）] カラム	Warning の最大しきい値。
[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。

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 [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 [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 サーバの温度に関する次の統計情報が表示されます。

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
[センサーのステータス（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） • Non-Recoverable
[気温（Temperature）]カラム	現在の温度（摂氏および華氏単位）。
[Warning 最小しきい値（Warning Threshold Min）] カラム	Warning の最小しきい値。
[Warning 最大しきい値（Warning Threshold Max）] カラム	Warning の最大しきい値。
[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。

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 [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 [センサー（Sensors）]ペインの [電圧（Voltage）] タブをクリックします。

ステップ 4 サーバの電圧に関する次の統計情報が表示されます。

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。

[名前（Name）]	説明
[センサー名（Sensor Name）] カラム	センサーの名前。
[ステータス（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） • Non-Recoverable
[電圧（Voltage）]カラム	現在の電圧（ボルト単位）。
[Warning 最小しきい値（Warning Threshold Min）] カラム	Warning の最小しきい値。
[Warning 最大しきい値（Warning Threshold Max）] カラム	Warning の最大しきい値。
[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。

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 [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 [センサー（Sensors）]ペインの [電流（Current）] タブをクリックします。

ステップ 4 電流に関する次の統計情報が [電流（Current）]タブに表示されます。

[名前（Name）]	説明
[センサー名（Sensor Name）] カラム	センサーの名前。
[ステータス（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） • Non-Recoverable
[電流（Current）]カラム	電流（アンペア単位）。
[Warning 最小しきい値（Warning Threshold Min）] カラム	Warning の最小しきい値。
[Warning 最大しきい値（Warning Threshold Max）] カラム	Warning の最大しきい値。
[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。

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 [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 [センサー（Sensors）]ペインの [LED] タブをクリックします。

ステップ 4 サーバの LED に関する次の統計情報が表示されます。

[名前（Name）]	説明
[センサー名（Sensor Name）] カラム	センサーの名前。
[LED の状態（LED State）]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 [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 [センサー（Sensors）]ペインの [ストレージ（Storage）] タブをクリックします。

ステップ 4 サーバのストレージに関する次の統計情報が表示されます。

[名前（Name）]	説明
[名前（Name）]カラム	ストレージ デバイスの名前。

[名前（Name）]	説明
[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。
[LED ステータス（LED Status）]カラム	現在の LED の色（該当する場合）。 ストレージ デバイスの物理 LED を点滅させるには、ドロップダウン リストから [オンにする（Turn On）]を選択します。LED の点滅をストレージ デバイスに制御させるには、[オフにする（Turn Off）]を選択します。 （注） この情報は、一部の C シリーズ サーバのみで使用できます。

第 6 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。

Configuring Serial Over LAN

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、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 [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 [リモート プレゼンス（Remote Presence）] 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 [Serial over LAN] タブをクリックします。

ステップ 4 [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。

[名前（Name）]	説明
[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
[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。
[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、Cisco IMC シェルを迂回して SoL にダイレクト アクセスできます。 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 5 [変更の保存（Save Changes）]をクリックします。

Configuring Virtual Media

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 [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 [リモート プレゼンス（Remote Presence）] 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 [仮想メディアのプロパティ（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を有効にする（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 の有効化（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、NIC が Cisco Card モードである場合には、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 [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 [リモート プレゼンス（Remote Presence）] 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 [仮想メディア（Virtual Media）] タブをクリックします。

ステップ 4 [Cisco IMC マップされた vMedia（Cisco IMC-Mapped vMedia）] 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 5 [Cisco IMC マップされた vMedia（Cisco IMC-Mapped vMedia）] 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 を使用する場合は、ポート 445（CIFS 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。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]：CommonInternet 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	マッピングするイメージの 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 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。オプションは選択した [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。 ◦ None：認証を使用しません。 ◦ 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 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 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、次のように入力します。 • 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	選択したユーザ名のパスワード（必要な場合）。

ステップ 6 [保存（Save）]をクリックします。

Cisco IMCマップされた vMedia ボリュームのプロパティの表示

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 [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 [リモート プレゼンス（Remote Presence）] 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 [仮想メディア（Virtual Media）] タブをクリックします。

ステップ 4 [Cisco IMC マップされた vMedia（Cisco IMC-Mapped vMedia）] 領域で、[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 5 [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
[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。 • [NFS]：ネットワークファイル システム。 • [CIFS]：CommonInternet 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。
[リモート共有（Remote Share）] フィールド	マッピングするイメージの URL。
[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。
[マウント オプション（Mount Options）]フィールド	選択されたマウント オプション。
[ユーザ名（User Name）]フィールド	ユーザ名（ある場合）。
[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（ある場合）。

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 [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 [リモート プレゼンス（Remote Presence）] 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 [仮想メディア（Virtual Media）] タブをクリックします。

ステップ 4 [Cisco IMC マップされた vMedia（Cisco IMC-Mapped vMedia）] 領域で、[マップ解除（Unmap）] をクリックします。
マッピングの保存を求めるプロンプトが表示されたら、[保存（Save）]をクリックします。

既存の Cisco IMC vMedia イメージのリマッピング

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 [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 [リモート プレゼンス（Remote Presence）] 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 [仮想メディア（Virtual Media）] タブをクリックします。

ステップ 4 [Cisco IMC マップされた vMedia（Cisco IMC-Mapped vMedia）]領域で、[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 5 [リマッピング（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 [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 [リモート プレゼンス（Remote Presence）] 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 [仮想メディア（Virtual Media）] タブをクリックします。

ステップ 4 [Cisco IMC マップされた vMedia（Cisco IMC-Mapped vMedia）]領域で、[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 5 [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。

Configuring the Virtual KVM

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 [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 [リモート プレゼンス（Remote Presence）] 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 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。
[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。
[ビデオの暗号化を有効にする（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を有効にする（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 5 [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 [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 [リモート プレゼンス（Remote Presence）] 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 で、[有効化（Enable）]チェックボックスをオンにします。

ステップ 5 [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 [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 [リモート プレゼンス（Remote Presence）] 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 で、[有効化（Enable）]チェックボックスをオフにします。

ステップ 5 [変更の保存（Save Changes）]をクリックします。

第 7 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。

Configuring Local Users

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）]タブに表示される [強力なパスワードの無効化（Disable Strong Password）] ボタンを使用すると、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。

リリース 2.0(9f) では、すべてのローカル ユーザを無効にし、LDAP や Active Directory などのリモート認証のみを使用して認証するように選択できます。これを可能にするため、ローカル ユーザ管理では、デフォルトの admin ユーザを含むすべての Cisco IMC ユーザの無効化をサポートしています。

警告 すべての Cisco IMC ユーザの無効化を選択し、Cisco IMC にログオンする代替方法がない場合は、Cisco IMC にアクセスできない場合があります。回避策として、Cisco IMC のファクトリー デフォルトが必要です。これにより、デフォルトの admin ユーザ クレデンシャルが有効になります。

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）] 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 [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、行をクリックします。

ステップ 5 [ユーザの詳細（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	ユーザの固有識別子。
[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。 ◦ 電源オン、電源再投入、電源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 • [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アイコン上にカーソルを移動すると、パスワードの設定に関する次のような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。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 [変更の保存（Save Changes）]をクリックします。

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ことで、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。

Configuring the LDAP Server

ユーザ認証および許可に LDAP を使用するように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

プロパティ（Properties）	値
構文	Case Sensitive String

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 [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) [Attributes]タブをクリックして、[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"
読み取り専用（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）] 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）]領域で、次のプロパティを更新します。

[名前（Name）]	説明
[LDAP を有効にする（Enable LDAP）]チェックボックス	オンにすると、最初に 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が処理されます。
[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 サーバの場合、これは dc=domain,dc=com 形式です。
[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を有効にする（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）の秒数（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。
[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 データベースと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）]

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	オンにすると、Active Directory は事前設定された LDAP サーバを使用します。
[LDAP サーバ（LDAP Servers）]のフィールド	
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、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 台の LDAP サーバを設定できます。 （注） ホスト名の IP アドレスを指定することもできます。
[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 ポートを介して行われます。グローバル カタログ サーバへの LDAPS 通信は TCP 3269 ポートを介して行われます。
[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）]のフィールド	

[名前（Name）]	説明
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の使用を指定します。 • [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ではなく、ログインID から抽出された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。 ソースを [抽出済み（Extracted）]に指定した場合、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。 ソースを [抽出済み（Extracted）]に指定した場合、このフィールドは無効になります。

ステップ 6　[バインド 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。このオプションを選択し、LDAPサーバで匿名ログインが設定されている場合は、ユーザのアクセスが可能です。 • [設定済みクレデンシャル（Configured Credentials）] : 初期バインドプロセスで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 プロセスで再利用されます。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[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[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で [グループの設定（Configure Group）] ボタンが有効になります。

[名前（Name）]	説明
[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。
[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、LDAP サーバ データベース内のグループの名前。
[グループのドメイン（Group Domain）]カラム	グループが属する必要がある LDAP サーバのドメイン。
[ロール（Role）]カラム	この LDAP サーバ グループのすべての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。 ◦ 電源オン、電源再投入、電源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 • [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の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。

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。

ローカル ブラウザからの 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 [証明書（Certificate）]領域で、[ローカル ブラウザからの LDAP CA 証明書のダウンロード（Download LDAP CA Certificate from Local Browser）] リンクをクリックします。
[ローカル ブラウザからの LDAP CA 証明書のダウンロード（Download LDAP CA Certificate from Local Browser）]ダイアログボックスが表示されます。

[名前（Name）]	説明
[ファイル（File）]フィールド	[参照（Browse）]ボタンを使用して、Cisco IMC GUI を実行するコンピュータのローカル ドライブに保存された LDAP CA 証明書を選択します。
[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。

リモート サーバからの 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 [証明書（Certificate）]領域で、[リモート サーバからの LDAP CA 証明書のダウンロード（Download LDAP CA Certificate from Remote Server）] リンクをクリックします。
[リモート サーバからの LDAP CA 証明書のダウンロード（Download LDAP CA Certificate from Remote Server）]ダイアログボックスが表示されます。

[名前（Name）]	説明
[LDAP CA 証明書のダウンロード元（Download LDAP CA Certificate from）]ドロップダウン リスト	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） リモート サーバ タイプとして SCP または SFTP を選択してこのアクションを実行した場合、ポップアップ ウィンドウに「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存するサーバの 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。 • [ユーザ名（Username）]フィールド：システムがリモート サーバへのログイン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。

[名前（Name）]	説明
[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 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 [証明書（Certificate）]領域で、[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 サーバへの LDAP CA 証明書のエクスポート（Export LDAP CA Certificate to Remote Server）	

[名前（Name）]	説明
	このオプションを選択することで、リモートサーバから証明書を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） リモート サーバ タイプとして SCP または SFTP を選択してこのアクションを実行した場合、ポップアップ ウィンドウに「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。 • [ユーザ名（Username）] フィールド：シス

[名前（Name）]	説明
	テムがリモート サーバへのログイン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。
ローカル ファイルへの LDAP CA 証明書のエクスポート（Export LDAP CA Certificate 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。

ステップ 5 [エクスポート（Export）]をクリックします。

LDAP CA 証明書の貼り付け

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 [証明書（Certificate）]領域で、[LDAP CA 証明書の貼り付け（Paste LDAP CA Certificate）] リンクをクリックします。

[LDAP CA 証明書の貼り付け（Paste LDAP CA Certificate）]ダイアログボックスが表示されます。

[名前（Name）]	説明
[証明書（Certificate）]テキストフィールド	署名付き証明書の内容全体をコピーして、ここに貼り付けます。 （注） ダウンロードする前に証明書が署名済みであることを確認してください。

ステップ 5 [証明書の保存（Save Certificate）]をクリックします。

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を有効にする（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 [証明書（Certificate）]領域で、[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。

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）] 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 [セッション（Sessions）] タブをクリックします。

ステップ 4 現在のユーザ セッションに関する次の情報が表示されます。

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。

[名前（Name）]	説明
[セッション ID（Session ID）] カラム	セッションの固有識別子。
[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。

パスワードの有効期限切れ

期限が切れた後のパスワードの保存期限を設定できます。管理者は日単位でこの期間を設定できます。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、ログイン時にユーザに通知され、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） 以前のデータベースにダウングレードすると、既存のユーザは削除されます。データベースはデフォルト設定に戻ります。以前に設定したユーザがクリアされ、データベースが空になるため、データベースに存在するのはデフォルトのユーザ名「admin」とパスワード「password」です。サーバにデフォルトのユーザデータベースが残っているため、デフォルトクレデンシャルの変更機能は有効です。つまり、ダウングレード後初めてデータベースにログインする際に、「admin」ユーザは必ずデフォルト クレデンシャルを変更する必要があります。

パスワード設定時刻

すべての既存ユーザの「パスワード設定時刻」は、移行またはアップグレードを行った時刻に設定されます。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た時刻に設定され、パスワードが設定されます。一般ユーザ（新規および既存）の「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

- パスワードの期限切れ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）] 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 [ローカル ユーザ（Local Users）]ペイン（デフォルトで開いています）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
[パスワードの期限切れを有効にする（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	既存のパスワードが期限切れになるように設定できる期間（新しいパスワードを設定した時点、または既存のパスワードを変更した時点からの期間）。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。有効にした場合は、パスワードを繰り返し使うことができません。0 ～ 5 の間の値を入力します。0 を入力すると、このフィールドは無効になります。
[通知期間（Notification Period）] フィールド	パスワードの期限が切れる時期を通知します。0 ～ 15 日の範囲内の値を入力します。0 を入力すると、このフィールドは無効になります。
[猶予期間（Grace Period）] フィールド	期限切れ後も既存のパスワードを使用できる期間。0 ～ 5 日の範囲内の値を入力します。0 を入力すると、このフィールドは無効になります。

ステップ 5 [変更の保存（Save Changes）]をクリックします。

パスワードの期限切れの有効化

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）] 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 [ローカル ユーザ（Local Users）]領域（デフォルトで開いています）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、[パスワードの期限切れを有効にする（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、日単位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。

第 8 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 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。
- [共有 LOM（Shared LOM）]：Cisco IMCへのアクセスに使用できる LOM（LAN on Motherboard）ポート。

- [共有 LOM 10G（Shared LOM 10G）]：どの 10G LOM ポートも、Cisco IMC へのアクセスに使用できます。
- [CiscoCard]：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。
- [共有 LOM 拡張（SharedLOM Extended）]：Cisco IMC へのアクセスに使用できる LOM ポートまたはアダプタ カードのポート。Cisco アダプタ カードは NCSI サポートのあるスロットに取り付ける必要があります。

（注） [共有 LOM 拡張（Shared LOM Extended）]および [共有 LOM 10G（Shared LOM 10G）] は、一部の UCS C シリーズ サーバでのみ使用できます。

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。

- [なし（none）]：設定されているNICモードに関連付けられた各ポートは個別に動作します。問題が発生した場合、ポートはフェールオーバーしません。
- [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は同時に動作します。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。

（注） [アクティブ-アクティブ（active-active）]を使用する場合は、メンバーインターフェイスのアップストリーム スイッチに port-channel を設定しないでください。port-channel は、[アクティブ-スタンバイ（active-standby）]を使用する場合に設定できます。

- [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、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 VLAN 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 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）] タブをクリックします。

ステップ 2 [管理者（Admin）] タブの [ネットワーク（Network）] をクリックします。

ステップ 3 [ネットワーク（Network）]ペインの [ネットワーク設定（Network Settings）] タブをクリックします。

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

[名前（Name）]	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。 • [共有 LOM（Shared LOM）]：Cisco IMCへのアクセスに使用できる LOM（LAN on Motherboard）ポート。 • [共有 LOM 10G（Shared LOM 10G）]：どの 10G LOM ポートも、Cisco IMC へのアクセスに使用できます。 • [CiscoCard]：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。 • [共有 LOM 拡張（SharedLOM Extended）]：Cisco IMC へのアクセスに使用できる LOM ポートまたはアダプタ カードのポート。Cisco アダプタ カードは NCSI サポートのあるスロットに取り付ける必要があります。 （注） [共有 LOM 拡張（Shared LOM Extended）]および [共有 LOM 10G（Shared LOM 10G）] は、一部の UCS C シリーズ サーバでのみ使用できます。 （注） いずれかの共有 LOM オプションを選択した場合は、すべてのホスト ポートが同じサブネットに属することを確認してください。

[名前（Name）]	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 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。
[SIOC スロット（SIOC Slot）] ドロップダウン リスト	Cisco IMC ネットワーク モードを設定します。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 モードを Cisco カード モードまたは共有 LOM モードに変更できます。 （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Cisco IMC
[NIC 冗長性（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。 • [なし（none）]：設定されているNIC モードに関連付けられた各ポートは個別に動作します。問題が発生した場合、ポートはフェールオーバーしません。 • [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は同時に動作します。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。 （注） [アクティブ-アクティブ（active-active）]を使用する場合は、メンバー インターフェイスのアップストリーム スイッチにport-channelを設定しないでください。port-channel は、[アクティブ-スタンバイ（active-standby）]を使用する場合に設定できます。 • [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、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 VLAN 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 5 [変更の保存（Save Changes）]をクリックします。

共通プロパティ設定

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で利用でき、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 UpdateDomain）]：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）] タブをクリックします。

ステップ 2 [管理者（Admin）] タブの [ネットワーク（Network）] をクリックします。

ステップ 3 [ネットワーク（Network）]ペインの [ネットワーク設定（Network Settings）] タブをクリックします。

ステップ 4 [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) [ホスト名（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、送信される 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 5 [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）] タブをクリックします。

ステップ 2 [管理者（Admin）] タブの [ネットワーク（Network）] をクリックします。

ステップ 3 [ネットワーク（Network）]ペインの [ネットワーク設定（Network Settings）] タブをクリックします。

ステップ 4 [IPv4 のプロパティ（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。
[IPアドレス（IP Address）] フィールド	Cisco IMCの 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。
[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 5 [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）] タブをクリックします。

ステップ 2 [管理者（Admin）] タブの [ネットワーク（Network）] をクリックします。

ステップ 3 [ネットワーク（Network）]ペインの [ネットワーク設定（Network Settings）] タブをクリックします。

ステップ 4 [IPv6 のプロパティ（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。
[IPアドレス（IP Address）] フィールド	Cisco IMCの 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。
[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。

[名前（Name）]	説明
[ステートレス アドレス自動設定（Stateless Address Auto Configuration）]フィールド	ステートレスアドレス自動設定（SLAAC）は、ネットワークのルータ アドバタイズメント（RA）によって決まります。

ステップ 5 [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）] タブをクリックします。

ステップ 2 [管理者（Admin）] タブの [ネットワーク（Network）] をクリックします。

ステップ 3 [ネットワーク（Network）]ペインの [ネットワーク設定（Network Settings）] タブをクリックします。

ステップ 4 [VLAN のプロパティ（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 5 [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

（注） ポートプロファイルまたはVLANを設定できますが、両方を使用することはできません。ポート プロファイルを使用する場合は、[VLAN のプロパティ（VLAN Properties）]領域の [VLAN の有効化（Enable VLAN）] チェックボックスがオフになっていることを確認します。

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）] タブをクリックします。

ステップ 2 [管理者（Admin）] タブの [ネットワーク（Network）] をクリックします。

ステップ 3 [ネットワーク（Network）]ペインの [ネットワーク設定（Network Settings）] タブをクリックします。

ステップ 4 [ポート プロファイル（Port Profile）]領域で、次のプロパティを更新します。

[名前（Name）]	説明
[ポートプロファイル（Port Profile）]フィールド	Cisco UCS VIC 1225 仮想インターフェイス カードなど、サポートされているアダプタ カード上の管理インターフェイス、仮想イーサネット、および VIF を設定するために Cisco IMC が使用するポート プロファイル。 最大 80 文字の英数字で入力します。-（ハイフン）と _（アンダースコア）を除き、スペースなどの特殊文字は使用できません。ポートプロファイル名をハイフンで始めることもできません。 （注） ポート プロファイルは、このサーバが接続されているスイッチに定義されている必要があります。

ステップ 5 [変更の保存（Save Changes）]をクリックします。

インターフェイス プロパティの設定

ネットワーク インターフェイス設定の概要

Cisco IMC管理ポートのネットワーク速度とデュプレックスモードを設定するために、このサポートが追加されています。自動ネゴシエーション モードは、専用モードでのみ設定できます。自動ネゴシエーションを有効にすると、ネットワーク ポート速度とデュプレックスの設定がシステムによって無視され、Cisco IMC がスイッチに設定された速度を保持します。自動ネゴシエーションを無効にする場合は、ネットワーク ポート速度（10 Mbps、100 Mbps、または1 Gbps）を設定し、デュプレックス値をフルまたはハーフで設定できます。

ポート プロパティは次の 2 つのモードで管理できます。

- [管理モード（AdminMode）] : [自動ネゴシエーション（Auto Negotiation）]オプションを無効にすることで、ネットワーク速度とデュプレックス値を設定できます。管理モードでのネットワーク速度のデフォルト値は 100 Mbps で、デュプレックス モードは [フル（Full）] に設定されます。ネットワーク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。
- [操作モード（OperationMode）] : 運用ネットワークのポート速度とデュプレックス値が表示されます。自動ネゴシエーションモードを有効にした場合は、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。

Cisco IMC1.5(x)、2.0(1)、および2.0(3) バージョンを工場出荷時の初期状態にリセットすると、[共有 LOM（Shared LOM）] モードがデフォルトで設定されます。

C3160 サーバの場合、工場出荷時の初期状態にリセットすると、[専用（Dedicated）]モードが [フル（Full）] デュプレックス モードに設定され、速度はデフォルトで 100 Mbps になります。

インターフェイス プロパティの設定

速度またはデュプレックスの不一致を回避するために、スイッチの設定をCisco IMC設定と一致させる必要があります。

重要 このアク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。

手順

ステップ 1 Cisco IMCWeb UI にログインします。

ステップ 2 [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 3 [管理者（Admin）] タブの [ネットワーク（Network）] をクリックします。

ステップ 4 [ネットワーク（Network）]ペインの [ネットワーク設定（Network Settings）] タブをクリックします。

ステップ 5 [NIC のプロパティ（NIC Properties）]領域で、[NIC モード（NIC Mode）] ドロップダウン リストから [専用（Dedicated）] モードを選択します。
ネット速度、デュプレックスなどのネットワーク構成を設定するには、NIC モードを専用にする必要があります。

ステップ 6 [ポート プロパティ（Port Properties）]領域で次の手順を実行します。

- [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、デュプレックスの設定はシステムによって無視されます。Cisco IMCは、スイッチで設定された速度を保持します。
- [自動ネゴシエーション（Auto Negotiation）]チェックボックスをオフにすると、デュプレックスを設定できます。設定しない場合、デフォルト速度 100 Mbps が適用され、以前のデュプレックスの値が保持されます。

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。

ステップ 7 [変更の保存（Save Changes）]をクリックします。

Network Security Configuration

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）] タブをクリックします。

ステップ 2 [管理者（Admin）] タブの [ネットワーク（Network）] をクリックします。

ステップ 3 [ネットワーク（Network）]ペインの [ネットワーク セキュリティ（Network Security）] タブをクリックします。

ステップ 4 [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 ブロッキングを有効にする（Enable IP Blocking）]チェックボックス	IP ブロッキ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 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。 この回数のログイン試行の失敗は、[IP ブロッキングの失敗期間（IP Blocking Fail Window）]フィールドで指定されている期間内に発生する必要があります。 3 ～ 10 の整数を入力します。
[IP ブロッキングの失敗期間（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 5 [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 フィルタリングを有効にする（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。

[名前（Name）]	説明
[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ます。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）を指定します。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することはできなくなります。

ステップ 6 [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 サービスを導入すれば、NTP サーバと時刻を同期するようにCisco IMCを設定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。

Configuring Network Time Protocol Settings

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）] タブをクリックします。

ステップ 2 [管理者（Admin）] タブの [ネットワーク（Network）] をクリックします。

ステップ 3 [ネットワーク（Network）]ペインの [NTP 設定（NTP Settings）] タブをクリックします。

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。
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）に同期されます（synchronized to NTP server (RefID) at stratum7）]：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。 • [同期されません（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 サービスが無効です（NTP service disabled）]：NTP サービスが無効な場合。

ステップ 5 [変更の保存（Save Changes）]をクリックします。

Web UI からの IP アドレスの ping

このリリースでは、ツールバーに表示される [Ping]ボタンを使用して、Cisco IMC Web UI から IP アドレスの ping を実行できるようになりました。これは、Cisco IMC で使用できる IP アドレスへのネットワーク接続の検証に役立ちます。このボタンを使用して、IPv4、IPv6、またはホスト IP アドレスの ping 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、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 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。

[名前（Name）]	説明
[ホスト名/IP アドレス（Hostname/IP Address）]カラム	送信先のホスト名または IP アドレス。
[再試行回数（Number of Retries）]カラム	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）]カラム	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）]領域	ping の結果を表示します。

ステップ 3 [Ping]をクリックします。

第 9 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。

Cisco UCS C シリーズ ネットワーク アダプタの概要

（注） この章の手順は、Cisco UCS C シリーズ ネットワーク アダプタがシャーシに設置される場合にのみ使用できます。

Cisco UCS C シリーズ ネットワーク アダプタを設置することで、I/O の統合と仮想化をサポートするためのオプションが提供されます。次のアダプタを使用できます。

- Cisco UCS P81E 仮想インターフェイス カード
- Cisco UCS VIC 1225 仮想インターフェイス カード
- Cisco UCS VIC 1385 仮想インターフェイス カード
- Cisco UCS VIC 1227T 仮想インターフェイス カード

- Cisco UCS VIC 1387 仮想インターフェイス カード

対話型の *UCS* ハードウェアおよびソフトウェア相互運用性ユーティリティを使用すると、選択したサーバモデルとソフトウェア リリース用のサポートされているコンポーネントと構成を表示できます。このユーティリティは次の URL で入手できます。http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html

Cisco UCS P81E 仮想インターフェイス カード

Cisco UCS P81E 仮想インターフェイス カードは、仮想化された環境、物理環境のモビリティ強化を求めている組織、および NIC、HBA、ケーブル配線、スイッチの減少によるコスト削減と管理オーバーヘッドの軽減を目指しているデータセンター向けに最適化されています。Fibre Channel over Ethernet（FCoE）PCIe カードには、次の利点があります。

- ジャストインタイムのプロビジョニングを使用して、最大で 16 個の仮想ファイバ チャネルと 16 個の仮想イーサネット アダプタを仮想化または非仮想化環境でプロビジョニングできます。それにより、システムの柔軟性が大幅に向上するとともに、複数の物理アダプタを統合することが可能になります。
- Cisco VN-Link テクノロジーとパススルー スイッチングのハードウェアベースの実装を含む、徹底した仮想化のサポートが提供されます。
- ネットワーク ポリシーとセキュリティの可視性およびポータビリティが、仮想マシンにまでわたる全域で提供されることにより、システムのセキュリティおよび管理性が向上します。

仮想インターフェイス カードは、親ファブリック インターコネクトへの Cisco VN-Link 接続を確立します。これにより、仮想マシン内の仮想 NIC をインターコネクトの仮想インターフェイスに仮想リンクで接続できるようになります。Cisco Unified Computing System 環境では、仮想リンクを管理し、ネットワーク プロファイルを適用することができます。また、仮想マシンがシステム内のサーバ間を移動する際に、インターフェイスを動的に再プロビジョニングできます。

Cisco UCS VIC 1225 仮想インターフェイス カード

Cisco UCS VIC 1225 仮想インターフェイス カードは、サーバ仮想化によって導入される種々の新しい動作モードを高速化する、高性能の統合型ネットワーク アダプタです。優れた柔軟性、パフォーマンス、帯域幅を新世代の Cisco UCS C シリーズ ラックマウント サーバに提供します。

Cisco UCS VIC 1225 は、仮想ネットワーキングと物理ネットワーキングを単一のインフラストラクチャに統合する Cisco 仮想マシン ファブリック エクステンダ（VM-FEX）を実装しています。これにより、物理ネットワークから仮想マシンへのアクセスに対する可視性と、物理サーバと仮想サーバに対する一貫したネットワーク運用モデルの実現が可能になります。仮想化環境では、この詳細に設定できる自己仮想化アダプタにより、Cisco UCS C シリーズ ラックマウント サーバに統合モジュラ LAN インターフェイスが提供されます。その他の機能と特長には次のようなものがあります。

- 最大 256 台の PCIe 仮想デバイス、仮想ネットワーク インターフェイス カード（vNIC）または仮想ホストバス アダプタ（vHBA）のサポート、高い I/O 処理/秒（IOPS）、ロスレスイーサネットのサポート、サーバへの 20 Gbps の接続を提供。

- PCIe Gen2 x16 により、ファブリック インターコネクトへの冗長パスを通じてネットワーク集約型アプリケーションのホスト サーバに適切な帯域幅を確実に提供。
- シスコ認定のサードパーティ製アダプタ用にサーバのフルハイト スロットが確保されたハーフハイト設計。
- Cisco UCS Manager による一元管理。Microsoft Windows、Red Hat Enterprise Linux、SUSE Linux、VMware vSphere、および Citrix XenServer をサポート。

Cisco UCS VIC 1385 仮想インターフェイス カード

Cisco UCS VIC 1385 仮想インターフェイス カードは、デュアルポートの拡張型 Quad Small Form-Factor Pluggable（QSFP）40 ギガビット イーサネットおよび Fibre Channel over Ethernet（FCoE）対応のハーフハイト PCI Express（PCIe）カードで、Cisco UCS C シリーズ ラック サーバ専用に設計されています。包括的にさまざまな機能を提供するシスコの次世代統合型ネットワーク アダプタ（CNA）技術を採用しており、今後の機能ソフトウェア リリースに対して投資保護を実現します。このカードでは、ポリシーベースでステートレス、かつ俊敏性の高いサーバ インフラストラクチャを構築できます。このインフラストラクチャは、ネットワーク インターフェイス カード（NIC）またはホスト バス アダプタ（HBA）として動的に設定可能な、256 を超える PCIe 規格準拠インターフェイスをホストに提供します。さらに、Cisco UCS VIC 1385 カードは、Cisco UCS ファブリック インターコネクトのポートを仮想マシンまで拡張する Cisco Data Center Virtual Machine Fabric Extender（VM-FEX）テクノロジーをサポートしているため、サーバ仮想化の展開が容易になります。

カードの特性は、ブート時にサーバに関連付けられたサービス プロファイルを使用して動的に設定されます。サービス プロファイルでは、PCIe インターフェイスの番号、タイプ（NIC または HBA）、ID（MAC アドレスおよび World Wide Name（WWN））、フェールオーバー ポリシー、帯域幅、Quality of Service（QoS）ポリシーを定義できます。インターフェイスをオンデマンドで定義、作成、利用できるため、ステートレスで俊敏性の高いサーバ インフラストラクチャが実現します。その他の機能と特長には次のようなものがあります。

- VIC 上に作成された各 PCIe インターフェイスは、それぞれ Cisco UCS ファブリック インターコネクト上のインターフェイスに関連付けられ、VIC 上の PCIe デバイスとファブリック インターコネクト上のインターフェイスを結ぶ各仮想ケーブルは、それぞれ完全に分離して認識されます。
- Cisco UCS VIC 1385 仮想インターフェイス カードは高いネットワーク パフォーマンスに加え、SMB-Direct、VMQ、DPDK、Cisco NetFlow などの最も要求の厳しいアプリケーションに対する低遅延を実現します。

Cisco UCS VIC 1227T 仮想インターフェイス カード

Cisco UCS VIC 1227T 仮想インターフェイス カードは、デュアルポートの 10GBASE-T（RJ-45）10-Gbps イーサネットおよび Fibre Channel over Ethernet（FCoE）対応の PCI Express（PCIe）モジュラ LAN-on-motherboard（mLOM）アダプタで、Cisco UCS C シリーズ ラック サーバ専用に設計されています。シスコのラック サーバに新たに導入された mLOM スロットを使用すれば、PCIe スロットを使わずに Cisco VIC を装着できます。これにより、I/O 拡張性が向上します。シスコの次世代統合型ネットワーク アダプタ（CNA）技術が取り入れられており、低コストのツイスト ペア

ケーブルで、30 m までのビット エラー レート（BER）が 10 ～ 15 のファイバ チャネル接続を提供します。また、将来の機能リリースにおける投資保護を実現します。mLOM カードでは、ポリシーベースでステートレス、かつ俊敏性の高いサーバ インフラストラクチャを構築できます。このインフラストラクチャは、ネットワーク インターフェイス カード（NIC）またはホスト バス アダプタ（HBA）として動的に設定可能な、最大 256 の PCIe 規格準拠インターフェイスをホストに提供します。さらに、Cisco UCS VIC 1227T 仮想インターフェイス カードは、Cisco UCS ファブリック インターコネクトのポートを仮想マシンまで拡張する Cisco Data Center Virtual Machine Fabric Extender（VM-FEX）テクノロジーをサポートしているため、サーバ仮想化の展開が容易になります。その他の機能と特長には次のようなものがあります。

- ステートレスで俊敏性の高い設計：このカードの特性は、サーバブート時にサーバに関連付けられたサービス プロファイルを使用して動的に決定されます。サービス プロファイルでは、PCIe インターフェイスの番号、タイプ（NIC または HBA）、ID（MAC アドレスおよび World Wide Name（WWN））、フェールオーバー ポリシー、帯域幅、Quality of Service（QoS）ポリシーを定義できます。インターフェイスをオンデマンドで定義、作成、利用できるため、ステートレスで俊敏性の高いサーバ インフラストラクチャが実現します。
- VIC 上に作成された各 PCIe インターフェイスは、それぞれ Cisco UCS ファブリック インターコネクト上のインターフェイスに関連付けられ、VIC 上の PCIe デバイスとファブリック インターコネクト上のインターフェイスを結ぶ各仮想ケーブルは、それぞれ完全に分離して認識されます。
- Cisco SingleConnect テクノロジーは、データセンターのコンピューティングを接続、管理するためのきわめて簡単、効率的かつインテリジェントな方法を提供します。Cisco SingleConnect テクノロジーによって、データセンターがラック サーバとブレード サーバ、物理サーバ、仮想マシン、LAN、SAN、および管理ネットワークに接続される方法が著しく簡略化されます。

Cisco UCS VIC 1387 仮想インターフェイス カード

Cisco UCS VIC 1387 仮想インターフェイス カードは、デュアルポートの拡張型 Quad Small Form-Factor Pluggable（QSFP）40 ギガビット イーサネットおよび Fibre Channel over Ethernet（FCoE）対応のハーフハイト PCI Express（PCIe）カードで、Cisco UCS C シリーズ ラック サーバ専用に設計されています。包括的にさまざまな機能を提供するシスコの次世代統合型ネットワーク アダプタ（CNA）技術を採用しており、今後の機能ソフトウェア リリースに対して投資保護を実現します。このカードでは、ポリシーベースでステートレス、かつ俊敏性の高いサーバ インフラストラクチャを構築できます。このインフラストラクチャは、ネットワーク インターフェイス カード（NIC）またはホスト バス アダプタ（HBA）として動的に設定可能な、256 を超える PCIe 規格準拠インターフェイスをホストに提供します。さらに、Cisco UCS VIC 1387 カードは、Cisco UCS ファブリック インターコネクトのポートを仮想マシンまで拡張する Cisco Data Center Virtual Machine Fabric Extender（VM-FEX）テクノロジーをサポートしているため、サーバ仮想化の展開が容易になります。

カードの特性は、ブート時にサーバに関連付けられたサービス プロファイルを使用して動的に設定されます。サービス プロファイルでは、PCIe インターフェイスの番号、タイプ（NIC または HBA）、ID（MAC アドレスおよび World Wide Name（WWN））、フェールオーバー ポリシー、帯域幅、Quality of Service（QoS）ポリシーを定義できます。インターフェイスをオンデマンドで

定義、作成、利用できるため、ステートレスで俊敏性の高いサーバ インフラストラクチャが実現します。その他の機能と特長には次のようなものがあります。

- VIC 上に作成された各 PCIe インターフェイスは、それぞれ Cisco UCS ファブリック インターコネクト上のインターフェイスに関連付けられ、VIC 上の PCIe デバイスとファブリック インターコネクト上のインターフェイスを結ぶ各仮想ケーブルは、それぞれ完全に分離して認識されます。
- Cisco UCS VIC 1387 仮想インターフェイス カードは高いネットワーク パフォーマンスに加え、SMB-Direct、VMQ、DPDK、Cisco NetFlow などの最も要求の厳しいアプリケーションに対する低遅延を実現します。

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 [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 [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 [ネットワーク アダプタ（Network Adapters）] タブをクリックします。

ステップ 4 [ネットワーク アダプタ（Network Adapters）]領域で、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	アダプタが装着されているスロット。
[製品名（Product Name）]カラム	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。

ステップ 5 [アダプタ カード（Adapter Card）]領域で、次の情報を確認します。

[名前（Name）]	説明
[スロット（Slot）]カラム	ネットワーク アダプタが存在するスロット。
[製品名（Product Name）]カラム	ネットワーク アダプタの製品名。
[インターフェイスの数（Number of Interfaces）]カラム	ネットワーク 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）]カラム	
[ID]カラム	外部イーサネット インターフェイスの ID 番号。
[MAC アドレス（MAC Address）]カラム	外部イーサネット インターフェイスの MAC アドレス。

VIC 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。
- サポートされている仮想インターフェイスカード（VIC）がシャーシに装着されていて、サーバの電源がオン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 [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 [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 [Cisco VIC アダプタ（Cisco VIC Adapters）] タブをクリックします。

ステップ 4 [アダプタ カード（Adapter Cards）]領域で、プロパティを表示するアダプタをテーブル内でクリックします。
選択したアダプタのリソースが、[アダプタ カード（Adapter Cards）]領域の下のタブ付きメニューに表示されます。

ステップ 5 [アダプタ カード（Adapter Cards）]領域で、装着されているアダプタの次の情報を確認します。

[名前（Name）]	説明
[PCI スロット（PCI Slot）]カラム	アダプタが装着されている PCI スロット。
[製品名（Product Name）]カラム	アダプタの製品名。
[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。
[ベンダー（Vendor）]カラム	アダプタのベンダー。
[Cisco IMC 管理の有効化（Cisco IMC Management 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。

ステップ 6 [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューで、[一般（General）] タブをクリックします。

ステップ 7 [アダプタ カードのプロパティ（Adapter Card Properties）]領域で、アダプタの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	アダプタが装着されている PCI スロット。 （注） C220 M4 および C240 M4 サーバの場合、PCI スロットは [MLOM]としても表示される場合があります。
[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。

[名前（Name）]	説明
[ハードウェアのリビジョン（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、アダプタ設定が 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。
[説明（Description）]フィールド	ユーザが定義したアダプタの説明（存在する場合）。
[FIP モード（FIP Mode）] フィールド	FCoE Initialization Protocol（FIP）モードが有効になっているかどうか。FIP モードの場合、アダプタと現在の FCoE 標準との互換性が保たれます。
[LLDP]フィールド	LLDP オプションがこの VIC カードに対して有効になっているかどうか。 （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。
[VNTAG モード（VNTAG Mode）]フィールド	仮想ネットワーク タグ（VNTAG）が有効になっているかどうか。 VNTAG モードが有効になっている場合は、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 にポート プロファイルを関連付ける。 • 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。
[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。
[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。

ステップ 8 [外部イーサネット インターフェイス（External Ethernet Interfaces）]領域で、アダプタの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。
[リンク状態（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。
[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。 • Auto • 1 Gpbs • 10 Gpbs • 40 Gpbs （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
[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。 • Auto • 1 Gpbs • 10 Gpbs • 40 Gpbs （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。
[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。
[コネクタの存在（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）]：コネクタは存在しません。 （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。
[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。
[コネクタ部品番号（Connector Part Number）]カラム	コネクタの部品番号。 （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。

[名前（Name）]	説明
[コネクタ部品リビジョン（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。

ステップ 9 [ファームウェア（Firmware）]領域で、アダプタの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 [ファームウェアの有効化（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、その新しいファームウェアを手動で有効化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。
[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有効化のステータス。 （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。

次の作業

仮想 NIC および仮想 HBA のプロパティを表示するには、次の項を参照してください。

- vNIC のプロパティの表示, （194 ページ）

• vHBA のプロパティの表示, （178 ページ）

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 [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 [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 [ストレージ アダプタ（Storage Adapters）] 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	コントローラのタイプ。
[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。
[製品名（Product Name）] フィールド	アダプタの製品名。
[シリアル番号（Serial Number）]フィールド	アダプタのシリアル番号。
[ファームウェア パッケージ ビルド（Firmware Package Build）] フィールド	アダプタ用のインストール済みファームウェア パッケージ。
[製品ID（Product ID）]フィールド	アダプタの製品 ID。
[バッテリのステータス（Battery Status）]フィールド	アダプタのベンダー。
[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	アダプタの状態。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
[詳細（Details）]リンク	[詳細（Details）]リンクをクリックすると[ストレージ（Storage）]タブが表示されます。

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 カードでは、追加の vHBA を 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 [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 [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 [Cisco VIC アダプタ（Cisco VIC Adapters）] タブをクリックします。

ステップ 4 [アダプタ カード（Adapter Cards）] 領域でアダプタ カードを選択します。
サーバの電源が投入されている場合、選択したアダプタ カードのリソースが [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューに表示されます。

ステップ 5 [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューで、[vHBA] タブをクリックします。

ステップ 6 [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 を選択します。

ステップ 7 [プロパティ（Properties）]をクリックして [vHBA プロパティ（vHBA Properties）] ダイアログボックスを開きます。

ステップ 8 [一般（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。
[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。

[名前（Name）]	説明
[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。 MAC アドレスを自動的に生成するには、[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 VLAN がない場合は、[なし（NONE）]をクリックします。デフォルト VLAN がある場合は、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 の範囲の 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。
[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。 自動的に順序を設定するには、[任意（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。

[名前（Name）]	説明
[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 9 [エラーの修復（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 エラーの修復を有効にする（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 I/O 再試行回数（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。

[名前（Name）]	説明
[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 10 [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 11 [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
[I/O 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。

ステップ 12 [ファイバ チャネル ポートの 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。

[名前（Name）]	説明
[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 13 [ファイバ チャネル ポートの 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 14 [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 カウント（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 15 [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 [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 [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 [Cisco VIC アダプタ（Cisco VIC Adapters）] タブをクリックします。

ステップ 4 [アダプタ カード（Adapter Cards）] 領域でアダプタ カードを選択します。
サーバの電源が投入されている場合、選択したアダプタ カードのリソースが [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューに表示されます。

ステップ 5 [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューで、[vHBA] タブをクリックします。

ステップ 6 [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 を選択します。

ステップ 7 [プロパティ（Properties）]をクリックして [vHBA プロパティ（vHBA Properties）] ダイアログボックスを開きます。

ステップ 8 [一般（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。
[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。

[名前（Name）]	説明
[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。 MAC アドレスを自動的に生成するには、[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 VLAN がない場合は、[なし（NONE）]をクリックします。デフォルト VLAN がある場合は、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 の範囲の 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。
[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。 自動的に順序を設定するには、[任意（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。

[名前（Name）]	説明
[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 9 [エラーの修復（Error Recovery）]領域で、次のフィールドを更新します。

[名前（Name）]	説明
[FCP エラーの修復を有効にする（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。

[名前（Name）]	説明
[ポート ダウン I/O 再試行回数（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。
[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 10 [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 11 [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
[I/O 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。

ステップ 12 [ファイバ チャネル ポートの 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 13 [ファイバ チャネル ポートの 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 14 [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 カウント（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 15 [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 16 [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 [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 [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 [Cisco VIC アダプタ（Cisco VIC Adapters）] タブをクリックします。

ステップ 4 [アダプタ カード（Adapter Cards）] 領域でアダプタ カードを選択します。
サーバの電源が投入されている場合、選択したアダプタ カードのリソースが [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューに表示されます。

ステップ 5 [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューで、[vHBA] タブをクリックします。

ステップ 6 [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、[追加（Add）]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 [クローン（Clone）]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 7 [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 8 [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,（183 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 [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 [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 [Cisco VIC アダプタ（Cisco VIC Adapters）] タブをクリックします。

ステップ 4 [アダプタ カード（Adapter Cards）] 領域でアダプタ カードを選択します。
サーバの電源が投入されている場合、選択したアダプタ カードのリソースが [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューに表示されます。

ステップ 5 [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューで、[vHBA] タブをクリックします。

ステップ 6 [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 を選択します。

（注） デフォルトの 2 つの vHBA（[fc0]と [fc1]）は、どちらも削除することはできません。

ステップ 7 [削除（Delete）]をクリックし、[OK] をクリックして確定します。

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 [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 [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 [Cisco VIC アダプタ（Cisco VIC Adapters）] タブをクリックします。

ステップ 4 [アダプタ カード（Adapter Cards）] 領域でアダプタ カードを選択します。
サーバの電源が投入されている場合、選択したアダプタ カードのリソースが [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューに表示されます。

ステップ 5 [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューで、[vHBA] タブをクリックします。

ステップ 6 [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 を選択します。

ステップ 7 [ブート テーブル（Boot Table）]をクリックして、選択した vHBA の [ブート テーブル（Boot Table）] ダイアログボックスを開きます。

ステップ 8 [ブート テーブル（Boot Table）]ダイアログボックスで、[追加（Add）] 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 9 [ブート エントリの追加（Add Boot Entry）]ダイアログボックスで、次のフィールドを更新します。

[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 ポート名（WWPN）。 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	指定した場所をブート 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。

ステップ 10 [ブート エントリの追加（Add Boot Entry）]をクリックします。

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 [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 [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 [Cisco VIC アダプタ（Cisco VIC Adapters）] タブをクリックします。

ステップ 4 [アダプタ カード（Adapter Cards）] 領域でアダプタ カードを選択します。
サーバの電源が投入されている場合、選択したアダプタ カードのリソースが [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューに表示されます。

ステップ 5 [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューで、[vHBA] タブをクリックします。

ステップ 6 [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 を選択します。

ステップ 7 [ブート テーブル（Boot Table）]をクリックして、選択した vHBA の [ブート テーブル（Boot Table）] ダイアログボックスを開きます。

ステップ 8 [ブート テーブル（Boot Table）]ダイアログボックスで、削除するエントリをクリックします。

ステップ 9 [削除（Delete）]をクリックし、[OK] をクリックして確定します。

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 [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 [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 [Cisco VIC アダプタ（Cisco VIC Adapters）] タブをクリックします。

ステップ 4 [アダプタ カード（Adapter Cards）] 領域でアダプタ カードを選択します。
サーバの電源が投入されている場合、選択したアダプタ カードのリソースが [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューに表示されます。

ステップ 5 [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューで、[vHBA] タブをクリックします。

ステップ 6 [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 を選択します。

ステップ 7 [永続的なバインディング（Persistent Bindings）]をクリックして、選択した vHBA の [永続的なバインディング（Persistent Bindings）] ダイアログボックスを開きます。

ステップ 8 選択した vHBA の [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。
[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 9 [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構築

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 [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 [Cisco VIC アダプタ（Cisco VIC Adapters）] タブをクリックします。

ステップ 4 [アダプタ カード（Adapter Cards）] 領域でアダプタ カードを選択します。
サーバの電源が投入されている場合、選択したアダプタ カードのリソースが [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューに表示されます。

ステップ 5 [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューで、[vHBA] タブをクリックします。

ステップ 6 [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 を選択します。

ステップ 7 [永続的なバインディング（Persistent Bindings）]をクリックして、選択した vHBA の [永続的なバインディング（Persistent Bindings）] ダイアログボックスを開きます。

ステップ 8 選択した vHBA の [永続的なバインディング（Persistent Bindings）]ダイアログボックスで、[永続的なバインディングの再構築（Rebuild Persistent Bindings）] をクリックします。

ステップ 9 [閉じる（Close）]をクリックします。

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 カードでは、追加の vNIC を 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、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きわ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

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 のプロパティ（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。

[名前（Name）]	説明
[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。 アダプタに内部プールから使用可能な MAC アドレスを選択させるには、[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。
[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。

[名前（Name）]	説明
[PCI 順序（PCI Order）]フィールド	この vNIC が使用される順序。 自動的に順序を設定するには、[任意（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 VLAN がない場合は、[なし（NONE）]をクリックします。デフォルト VLAN がある場合は、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 の範囲の 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。VLAN を [アクセス（ACCESS）]モードに設定すると、スイッチからタグ付きで送信され、指定のデフォルト VLAN（1 ～ 4094）から受信するフレームは、vNIC 経由でホスト OS に送信されるときにタグが削除されます。 （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 番目のオプション ボタンをクリックし、関連する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。

[名前（Name）]	説明
[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。
[NVGRE の有効化（Enable NVGRE）]チェックボックス	Generic Routing Encapsulation を使用した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。

[名前（Name）]	説明
[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
[割り込みカウント（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等しくする必要があります。 1 ～ 514 の整数を入力します。
[調停時間（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。 • [MIN]：システムは[調停時間（Coalescing Time）]フィールドに指定された時間待機してから、別の割り込みイベントを送信します。 • [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
[受信キューカウント（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
[送信キューカウント（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 カウント（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 セグメンテーション 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 の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 の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。
[大規模な受信の有効化（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。

[名前（Name）]	説明
[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 [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 [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 [Cisco VIC アダプタ（Cisco VIC Adapters）] タブをクリックします。

ステップ 4 [アダプタ カード（Adapter Cards）] 領域でアダプタ カードを選択します。
サーバの電源が投入されている場合、選択したアダプタ カードのリソースが [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューに表示されます。

ステップ 5 [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューで、[vNIC] タブをクリックします。

ステップ 6 [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。

ステップ 7 [プロパティ（Properties）]をクリックして [vNIC のプロパティ（vNIC Properties）] ダイアログボックスを開きます。

ステップ 8 [一般（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 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。 アダプタに内部プールから使用可能な MAC アドレスを選択させるには、[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。
[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。

[名前（Name）]	説明
[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。 自動的に順序を設定するには、[任意（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 VLAN がない場合は、[なし（NONE）]をクリックします。デフォルト VLAN がある場合は、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 の範囲の 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。VLAN を [アクセス（ACCESS）]モードに設定すると、スイッチからタグ付きで送信され、指定のデフォルト VLAN（1 ～ 4094）から受信するフレームは、vNIC 経由でホスト OS に送信されるときにタグが削除されます。 （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 番目のオプション ボタンをクリックし、関連する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。

[名前（Name）]	説明
[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。
[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 を使用した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。

[名前（Name）]	説明
[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 9 [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
[割り込みカウント（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等しくする必要があります。 1 ～ 514 の整数を入力します。
[調停時間（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。 • [MIN]：システムは[調停時間（Coalescing Time）]フィールドに指定された時間待機してから、別の割り込みイベントを送信します。 • [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。

[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。 • [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 10 [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 カウント（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 11 [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 カウント（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 12 [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 カウント（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。

[名前（Name）]	説明
[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 13 [RoCE プロパティ（RoCE Properties）]領域で、次のフィールドを更新します。

[名前（Name）]	説明
[RoCE]チェックボックス	RoCE プロパティを変更するには、このチェックボックスをオンにします。
[キュー ペア（1 ～ 8192）（Queue Pairs (1 - 8192)）] フィールド	アダプタごとのキュー ペアの数。1 ～ 8192 の整数を入力します。 この数値は 2 のべき乗の整数にすることをお勧めします。vNIC ごとのキュー ペアの値としては 2048 が推奨されます。この場合、アダプタごとに 4 つの vNIC を作成できます。Windows ドライバは内部で使用するために 2 つのキュー ペアを確保するため、有効な値の範囲は vNIC あたり 4 ～ 8192 のキュー ペアになります。
[メモリ領域（1 ～ 524288）（Memory Regions (1 - 524288)）]フィールド	アダプタあたりのメモリ領域の数。1 ～ 524288 の整数を入力します。この数値は2のべき乗の整数にすることをお勧めします。推奨値は 131072 です。 メモリ領域は主に運用チャネルのセマンティクスを送信するために使用されるため、アプリケーション要件を満たすのに十分なメモリ領域の数がサポートされる必要があります。
[リソース グループ（1～128）（Resource Groups (1 - 128)）] フィールド	アダプタごとのリソース グループの数。1 ～ 128 の整数を入力します。最適なパフォーマンスを得るには、この数値は、システムの CPU コアの数以上である、2 のべき乗の整数にすることをお勧めします。推奨値は 32 です。 リソース グループは WQ、RQ、CQ などのハードウェア リソースの合計数と、RDMA 機能をサポートするために必要となる、ホストで使用可能なプロセッサ コアの合計数に基づく割り込み回数を定義します。最大限のパフォーマンスを引き出すとともに、より有効な不均一メモリ アクセスを実現するために、ホストはコアごとに特定のリソース グループを割り当てます。

ステップ 14 [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 セグメンテーション 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 の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 の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。
[大規模な受信の有効化（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 15 [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。

[名前（Name）]	説明
[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。

ステップ 16 [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 つ備えています。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 [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 [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 [Cisco VIC アダプタ（Cisco VIC Adapters）] タブをクリックします。

ステップ 4 [アダプタ カード（Adapter Cards）] 領域でアダプタ カードを選択します。
サーバの電源が投入されている場合、選択したアダプタ カードのリソースが [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューに表示されます。

ステップ 5 [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューで、[vNIC] タブをクリックします。

ステップ 6 [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、[追加（Add）]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、既存の vNIC を選択し、[クローン（Clone）]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 7 [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 8 （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 9 [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, （201 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 [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 [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 [Cisco VIC アダプタ（Cisco VIC Adapters）] タブをクリックします。

ステップ 4 [アダプタ カード（Adapter Cards）] 領域でアダプタ カードを選択します。
サーバの電源が投入されている場合、選択したアダプタ カードのリソースが [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューに表示されます。

ステップ 5 [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューで、[vNIC] タブをクリックします。

ステップ 6 [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 7 [削除（Delete）]をクリックし、[OK] をクリックして確定します。

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 パケットを送受信するときにカーネルをバイパスすることで、データセンターの Cisco UCS サーバで実行されるソフトウェア アプリケーションのパフォーマンスを改善します。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ため、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 のメリットを引き出すためには、アプリケーションはソケットまたはその他の通信 API ではなく、Message Passing Interface（MPI）を使用する必要があります。

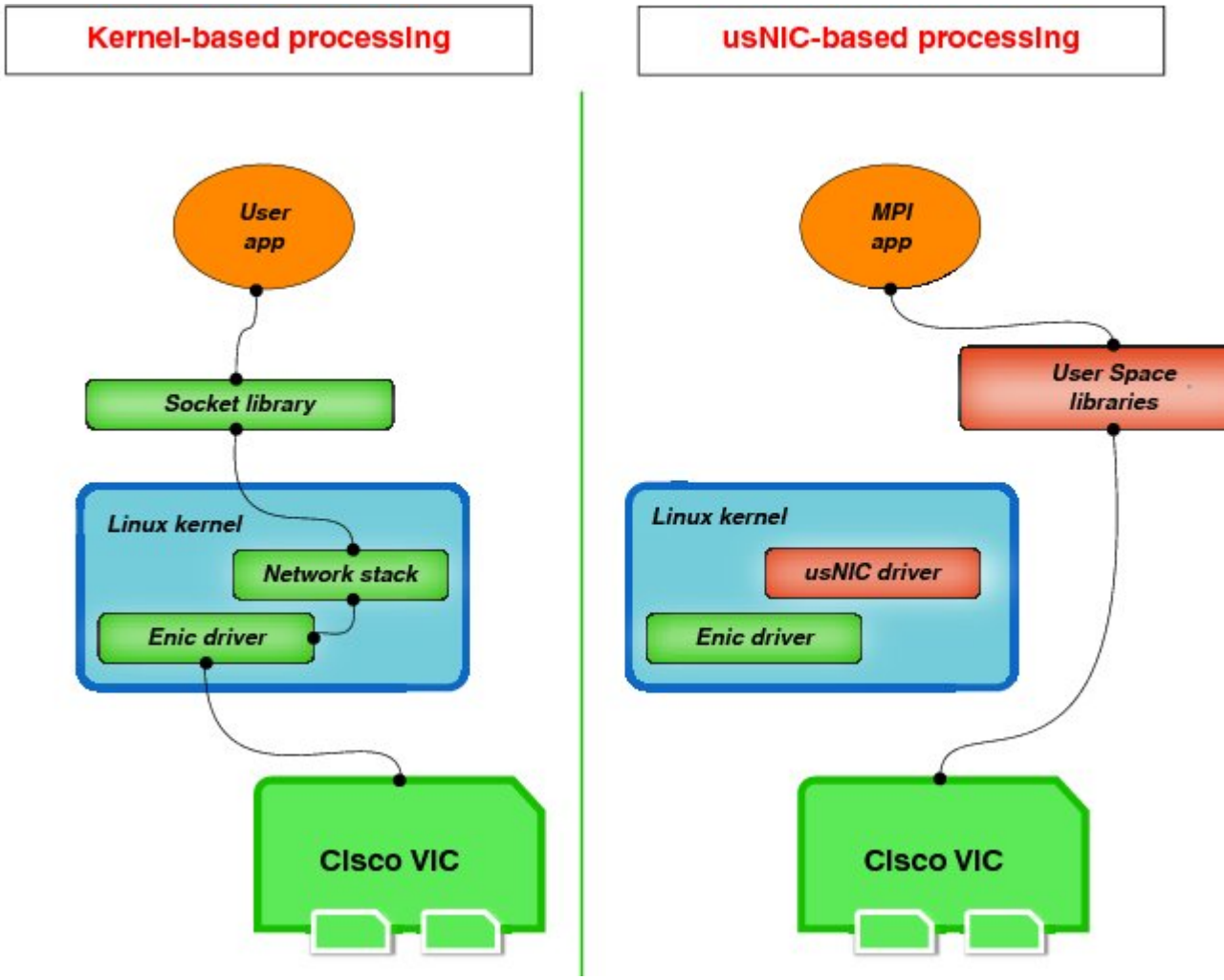
Cisco usNIC では、MPI アプリケーションに対して次の利点が得られます。

- 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 IMCGUI を使用した Cisco usNIC の設定

（注） [usNIC のプロパティ（usNIC properties）] ダイアログボックスには、Cisco usNIC の複数のプロパティが一覧表示されますが、次のプロパティのみを設定する必要があります。その他のプロパティは現在使用されていません。

- **cq-count**
- **rq-count**
- **tq-count**
- **usnic-count**

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 IMCGUI 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 を設定する方法を確認してください。

手順

ステップ 1 Cisco IMCGUI 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 [サーバ（Server）] タブをクリックします。

ステップ 3 [サーバ（Server）] タブの [インベントリ（Inventory）] をクリックします。

ステップ 4 [インベントリ（Inventory）]ペインの [Cisco VIC アダプタ（Cisco VIC Adapters）] タブをクリックします。

ステップ 5 [アダプタ カード（Adapter Cards）] 領域でアダプタ カードを選択します。
サーバの電源が投入されている場合、選択したアダプタ カードのリソースが [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューに表示されます。

ステップ 6 [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューで、[vNIC] タブをクリックします。

ステップ 7 [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） usNIC として設定する vNIC ごとに、テーブルから vNIC エントリを選択し、ステップ 9 ～ 18 の説明に従ってプロパティを指定します。

ステップ 8 [usNIC]をクリックして [usNIC のプロパティ（usNIC Properties）] ダイアログボックスを開きます。

ステップ 9 [usNIC（usNICs）]プロパティで、作成する Cisco usNIC の数を指定します。

サーバで実行されている各 MPI プロセスには、専用の usNIC が必要です。64 の MPI プロセスを同時に実行させるには、最大 64 の usNIC を作成する必要がある場合があります。usNIC 対応 vNIC ごとに、サーバの物理コアの数と同数の usNIC を最低限作成することを推奨します。たとえば、サーバに 8 つの物理コアがある場合は、8 つの usNIC を作成します。

ステップ 10 [プロパティ（Properties）]領域で、次のフィールドを更新します。

フィールド名	説明
送信キュー カウント（Transmit Queue Count）	割り当てる送信キュー リソースの数。 この値を 6 に設定することをお勧めします。
受信キュー カウント（Receive Queue Count）	割り当てる受信キュー リソースの数。 この値を 6 に設定することをお勧めします。
完了キューカウント（Completion Queue Count）	割り当てる完了キュー リソースの数。 この値を 6 に設定することをお勧めします。

ステップ 11 [適用（Apply）]をクリックします。

ステップ 12 [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 13 [サーバ（Server）] タブの[BIOS] をクリックします。

ステップ 14 [アクション（Actions）] 領域で[BIOS の設定（Configure BIOS）] をクリックします。

ステップ 15 ダイアログ ボックス で、[高度（Advanced）] タブをクリックします。

ステップ 16 [プロセッサの設定（Processor Configuration）]領域で、次のプロパティを [有効（Enabled）] に設定します。

- Intel(R) VT-d
- Intel(R) VT-d ATS サポート（Intel(R) VT-d ATS support）
- Intel(R) VT-d Coherency サポート（Intel(R) VT-d Coherency Support）

ステップ 17 [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 [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 [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 [Cisco VIC アダプタ（Cisco VIC Adapters）] タブをクリックします。

ステップ 4 [アダプタ カード（Adapter Cards）] 領域でアダプタ カードを選択します。
サーバの電源が投入されている場合、選択したアダプタ カードのリソースが [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューに表示されます。

ステップ 5 [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューで、[vNIC] タブをクリックします。

ステップ 6 [ホスト イーサネット インターフェイス（Host Ethernet Interface）]領域で、vNIC に割り当てられる usNIC を選択して [usNIC のプロパティ（usNIC properties）] ダイアログボックスを開きます。

ステップ 7 [usNIC]領域で、次のフィールドの情報を確認または更新します。

[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、既存の値よりも大きい値を入力します。 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。

ステップ 8 [プロパティ（Properties）]領域で、次のフィールドの情報を確認または更新します。

[名前（Name）]	**説明**
[送信キュー カウント（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。

[名前（Name）]	説明
[受信キュー カウント（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 カウント（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。
[割り込みカウント（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等しくする必要があります。 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。 • [MIN]：システムは[調停時間（Coalescing Time）] フィールドに指定された時間待機してから、別の割り込みイベントを送信します。 • [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の時間（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。

[名前（Name）]	説明
[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 セグメントのオフロード（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。
[大規模な受信（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。

[名前（Name）]	説明
[適用（Apply）]ボタン	vNIC デバイスに関連付けられたすべての usNIC に変更を適用します。
[値のリセット（Reset values）]ボタン	usNIC 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値に復元します。
[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。

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 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 [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 [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 [Cisco VIC アダプタ（Cisco VIC Adapters）]タブをクリックします。

ステップ 4 [アダプタ カード（Adapter Cards）] 領域でアダプタ カードを選択します。
サーバの電源が投入されている場合、選択したアダプタ カードのリソースが [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューに表示されます。

ステップ 5 [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューで、[vNIC] タブをクリックします。

ステップ 6 [ホストイーサネットインターフェイス（Host Ethernet Interfaces）]領域で、テーブルから vNIC を選択して [iSCSI ブート（iSCSI Boot）] をクリックします。

ステップ 7 [一般（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。
[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）。

[名前（Name）]	説明
[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 8 [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	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。 iSCSI イニシエータ名を定義する正規表現。 • .（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。
[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 サーバのアドレス。
[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。

[名前（Name）]	説明
[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 9 [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 10 [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。
[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。

[名前（Name）]	説明
[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 での iSCSI ブートを設定します。
[iSCSI の設定解除（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 11 [ISCSI の設定（Configure ISCSI）]をクリックします。

vNIC からの iSCSI ブート設定の削除

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 [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 [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 [Cisco VIC アダプタ（Cisco VIC Adapters）]タブをクリックします。

ステップ 4 [アダプタ カード（Adapter Cards）] 領域でアダプタ カードを選択します。
サーバの電源が投入されている場合、選択したアダプタ カードのリソースが [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューに表示されます。

ステップ 5 [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューで、[vNIC] タブをクリックします。

ステップ 6 [ホスト イーサネット インターフェイス（Host Ethernet Interfaces）]領域で、テーブルから vNIC を選択して [iSCSI ブート（iSCSI Boot）] をクリックします。

ステップ 7 表示されるダイアログボックスで [ISCSI の設定解除（Unconfigure ISCSI）]をクリックします。

vNIC の仮想マシン キューの設定

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。

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 [イーサネット インターフェイス（Ethernet Interfaces）]ペインの [vNIC のプロパティ（vNIC Properties）] 領域で、[VMQ の有効化（Enable VMQ）] チェックボックスをオンにします。

ステップ 4 [イーサネット送信キュー（Ethernet Transmit Queue）]領域で、[送信キュー カウント（Transmit Queue Count）]フィールドに整数を入力します。この数値は 1 より大きくする必要があります。

ステップ 5 [イーサネット受信キュー（Ethernet Receive Queue）]領域で、[受信キュー カウント（Receive Queue Count）]フィールドに整数を入力します。この数値は、送信キューの数と同じにする必要があります。

ステップ 6 [イーサネット割り込み（Ethernet Interrupt）]領域で、[割り込みカウント（Interrupt Count）]フィールドに整数を入力します。これは、論理プロセッサの数または完了キューの数と同じにする必要があります。

次の作業

- サーバをリブートします。
- NIC で論理スイッチを作成します。

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、次のいずれかのリモートサーバに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 [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 [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 [Cisco VIC アダプタ（Cisco VIC Adapters）] タブをクリックします。

ステップ 4 [アダプタ カード（Adapter Cards）] 領域でアダプタ カードを選択します。
サーバの電源が投入されている場合、選択したアダプタ カードのリソースが [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューに表示されます。

ステップ 5 [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューで、[一般（General）] タブをクリックします。

ステップ 6 [一般（General）]タブの [アクション（Actions）] 領域で、[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 7 [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。

[名前（Name）]	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） リモート サーバ タイプとして SCP または SFTP を選択してこのアクションを実行した場合、ポップアップ ウィンドウに「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 が使用する必要のあ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 8 [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 [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 [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 [Cisco VIC アダプタ（Cisco VIC Adapters）] タブをクリックします。

ステップ 4 [アダプタ カード（Adapter Cards）] 領域でアダプタ カードを選択します。
サーバの電源が投入されている場合、選択したアダプタ カードのリソースが [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューに表示されます。

ステップ 5 [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューで、[一般（General）] タブをクリックします。

ステップ 6 [一般（General）]タブの [アクション（Actions）] 領域で、[設定のインポート（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 7 [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。

[名前（Name）]	**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）** リモート サーバ タイプとして SCP または SFTP を選択してこのアクションを実行した場合、ポップアップ ウィンドウに「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。

[名前（Name）]	説明
[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。
[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 8 [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 サーバの指定されたパスから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 [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 [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 [Cisco VIC アダプタ（Cisco VIC Adapters）] タブをクリックします。

ステップ 4 [アダプタ カード（Adapter Cards）] 領域でアダプタ カードを選択します。
サーバの電源が投入されている場合、選択したアダプタ カードのリソースが [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューに表示されます。

ステップ 5 [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューで、[一般（General）] タブをクリックします。

ステップ 6 [一般（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。

アダプタ ファームウェアの管理

アダプタ ファームウェア

Cisco UCS C シリーズ ネットワーク アダプタには、次のファームウェア コンポーネントが含まれています。

- アダプタ ファームウェア：メインのオペレーティング ファームウェア（アクティブ イメージとバックアップ イメージで構成）は、Cisco IMCGUI インターフェイスか CLI インターフェイス、または Host Upgrade Utility（HUU）からインストールできます。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。

ローカル ファイルからのアダプタ ファームウェアのインストール

はじめる前に

アダプタ ファームウェア ファイルを管理コンピュータのファイル システムに保存します。

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 [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 [Cisco VIC アダプタ（Cisco VIC Adapters）] タブをクリックします。

ステップ 4 [アダプタ カード（Adapter Cards）] 領域でアダプタ カードを選択します。
サーバの電源が投入されている場合、選択したアダプタ カードのリソースが [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューに表示されます。

ステップ 5 [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューで、[一般（General）] タブをクリックします。

ステップ 6 [一般（General）]タブの [アクション（Actions）] 領域で、[ファームウェアのインストール（Install Firmware）] をクリックして [アダプタ ファームウェアのインストール（Install Adapter Firmware）] ダイアログボックスを開きます。

ステップ 7 [アダプタ ファームウェアのインストール（Install Adapter Firmware）]ダイアログボックスで、[ローカル ファイルからのインストール（Install from local file）] を選択し、[次へ（Next）] をクリックします。

ステップ 8 [参照...（Browse...）]をクリックし、アダプタ ファームウェア ファイルを見つけます。

ステップ 9 [ファームウェアのインストール（Install Firmware）]をクリックします。

次の作業

新しいファームウェアを有効化するには、「アダプタ ファームウェアの有効化」を参照してください。

リモート サーバからのアダプタ ファームウェアのインストール

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 [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 [Cisco VIC アダプタ（Cisco VIC Adapters）] タブをクリックします。

ステップ 4 [アダプタ カード（Adapter Cards）] 領域でアダプタ カードを選択します。
サーバの電源が投入されている場合、選択したアダプタ カードのリソースが [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューに表示されます。

ステップ 5 [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューで、[一般（General）] タブをクリックします。

ステップ 6 [一般（General）]タブの [アクション（Actions）] 領域で、[ファームウェアのインストール（Install Firmware）] をクリックして [アダプタ ファームウェアのインストール（Install Adapter Firmware）] ダイアログボックスを開きます。

ステップ 7 [アダプタ ファームウェアのインストール（Install Adapter Firmware）]ダイアログボックスで、[リモート サーバからのインストール（Install from Remote Server）] を選択し、[次へ（Next）] をクリックします。

ステップ 8 [アダプタ ファームウェアのインストール（Install Adapter Firmware）]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
[インストール元（Install 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） リモート サーバ タイプとして SCP または SFTP を選択してこのアクションを実行した場合、ポップアップ ウィンドウに「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 IP アドレスまたはホスト名。[インストール元（Install 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。
[戻る（Back）]ボタン	ファームウェア パッケージのローカル パスを指定する場合は、このボタンをクリックします。
[ファームウェアのインストール（Install Firmware）]ボタン	アダプタのバックアップ メモリ スロットに、選択したファームウェア パッケージをインストールするには、このボタンをクリックします。

[名前（Name）]	説明
[閉じる（Close）]ボタン	サーバに保存したファームウェアバージョンに変更を加えずにウィザードを終了するには、このボタンをクリックします。

ステップ 9 [ファームウェアのインストール（Install Firmware）]をクリックします。

次の作業

新しいファームウェアを有効化するには、「アダプタ ファームウェアの有効化」を参照してください。

アダプタ ファームウェアの有効化

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 [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 [Cisco VIC アダプタ（Cisco VIC Adapters）] タブをクリックします。

ステップ 4 [アダプタ カード（Adapter Cards）] 領域でアダプタ カードを選択します。
サーバの電源が投入されている場合、選択したアダプタ カードのリソースが [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューに表示されます。

ステップ 5 [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューで、[一般（General）] タブをクリックします。

ステップ 6 [一般（General）]タブの [アクション（Actions）] 領域で、[ファームウェアの有効化（Activate Firmware）] をクリックして [アダプタ ファームウェアの有効化（Activate Adapter Firmware）] ダイアログボックスを開きます。

ステップ 7 [アダプタ ファームウェアの有効化（Activate Adapter Firmware）]ダイアログボックスで、ファームウェアが次に起動するときに実行するイメージを選択します。

ステップ 8 [アダプタ ファームウェアの有効化（Activate Adapter Firmware）]をクリックします。

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 [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 [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 [Cisco VIC アダプタ（Cisco VIC Adapters）] タブをクリックします。

ステップ 4 [アダプタ カード（Adapter Cards）] 領域でアダプタ カードを選択します。
サーバの電源が投入されている場合、選択したアダプタ カードのリソースが [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューに表示されます。

ステップ 5 [アダプタ カード（Adapter Cards）] 領域の下のタブ付きメニューで、[一般（General）] タブをクリックします。

ステップ 6 [一般（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ます。

第 10 章

Managing Storage Adapters

この章の内容は、次のとおりです。

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

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）] タブをクリックします。

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 [ワーク（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 [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 5 [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。

- [Raid0]：単純なストライピング。
- [Raid1]：単純なミラーリング。
- [Raid5]：パリティ付きストライピング。
- [Raid6]：2 つのパリティ ドライブによるストライピング。
- [Raid10]：スパンされたミラーリング。
- [Raid50]：パリティ付きのスパンされたストライピング。
- [Raid60]：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 6 必要に応じて、[フル ディスク暗号化の有効化（Enable Full Disk Encryption）]チェックボックスを選択します。

これにより、ドライブ グループ上のディスクの暗号化が有効になり、保護することができます。

ステップ 7 [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。

ステップ 8 [仮想ドライブのプロパティ（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。
[ストリップ サイズ（Strip Size）]ドロップダウン リスト	各ストリップのサイズ（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。 • [ライト スルー（WriteThrough）]：データはキャッシュ経由で物理ドライブに書き込まれます。該当データの以降の読み取りをキャッシュから行えるため、パフォーマンスが改善されます。 • [ライトバック（WriteBack）]：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、[ライト スルー（Write Through）]キャッシングにフォールバックします。 • [不良 BBU のライト バック（WriteBack Bad BBU）]：このポリシーでは、バッテリ バックアップ ユニットに欠陥または放電があった場合も、書き込みキャッシングは [ライト 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（ReadWrite）]：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（ReadOnly）]：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 で読み取りおよび書き込みを実行できません。
[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 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）] タブをクリックします。

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 [ワーク（Work）]ペインで [コントローラ情報（Controller Info）] タブをクリックします。

ステップ 4 [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 5 [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 6 [仮想ドライブのプロパティ（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。
[ストリップ サイズ（Strip Size）]ドロップダウン リスト	各ストリップのサイズ（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。 • [ライト スルー（WriteThrough）]：データはキャッシュ経由で物理ドライブに書き込まれます。該当データの以降の読み取りをキャッシュから行えるため、パフォーマンスが改善されます。 • [ライト バック（WriteBack）]：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、[ライト スルー（Write Through）]キャッシングにフォールバックします。 • [不良 BBU のライト バック（WriteBack Bad BBU）]：このポリシーでは、バッテリ バックアップ ユニットに欠陥または放電があった場合も、書き込みキャッシングは [ライト 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（ReadWrite）]：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（ReadOnly）]：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 で読み取りおよび書き込みを実行できません。

[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 7 [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、[トランスポート準備の設定（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、すべての外部設定ルールが適用されます。ただし、トランスポート準備機能によって外部設定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 [ワーク（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、[トランスポート準備の設定（Set Transport Ready）] をクリックします。
[トランスポート準備の設定（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	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（ExludeAll）]：専用ホットスペア ドライブをすべて除外します。 • [すべて含む（IncludeAll）]：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 ドライブを含む（Include Dedicated Hot SpareDrive）]：排他的な専用ホットスペア ドライブを含めます。
[トランスポート準備の設定（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。

名前	説明
[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 [ワーク（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、[トランスポート準備の解除（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

セキュアなドライブ グループをホストする物理ドライブのセットが別のサーバまたはコントローラ（または、それらが存在しない間にセキュリティ キーが変更された同じコントローラ）に挿入されると、それらは外部設定になります。これらの外部設定は保護されているため、インポートする前に、セキュリティ キー情報を確認してロックを解除する必要があります。

外部設定のセキュリティ キーを確認して設定をインポートするには、次の手順を実行します。

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）] タブをクリックします。

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 [ワーク（Work）]ペインで [コントローラ情報（Controller Info）] タブをクリックします。

ステップ 4 [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。
これにより、[セキュア キー検証（Secure Key Verification）]ダイアログボックスが開きます。先に進む前に次の情報を確認します。

表 3 : [セキュア キー検証（*Secure Key Verification*）] 領域

[名前（Name）]	説明
[セキュリティ キー（Security Key）]フィールド	コントローラに割り当てられる一意のキー ID。
[確認（Verify）]ボタン	入力したキーが保存されているキー情報に一致するかどうかを確認します。 セキュア キーが正しいことが確認されると、要求したアクションが実行されます。
[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 [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がクリアされます。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）] タブをクリックします。
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 [ワーク（Work）]ペインで [コントローラ情報（Controller Info）] タブをクリックします。
ステップ 4 [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 5 [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）] タブをクリックします。
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 [ワーク（Work）]ペインで [コントローラ情報（Controller Info）] タブをクリックします。
ステップ 4 [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 5 [OK]をクリックして確認します。

JBOD のイネーブル化

（注） 一部の UCS C シリーズ サーバでのみ Just a Bunch Of Disks（JBOD）を有効にできます。

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 アダプタ（Storage Adapters）]ペインで、適切な MegaRAID コントローラをクリックします。

ステップ 3 [ワーク（Work）]ペインで [コントローラ情報（Controller Info）] タブをクリックします。

ステップ 4 [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 5 [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）] タブをクリックします。

ステップ 2 [ストレージ アダプタ（Storage Adapters）]ペインで、適切な MegaRAID コントローラをクリックします。

ステップ 3 [ワーク（Work）]ペインで [コントローラ情報（Controller Info）] タブをクリックします。

ステップ 4 [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 5 [OK]をクリックして確定します。

削除するドライブの準備

（注） [未設定良好（Unconfigured Good）]ステータスが表示される物理ドライブでのみ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）] タブをクリックします。

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 [ワーク（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、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。

コントローラの TTY ログの取得

このタスクは、コントローラの TTY ログを取得し、それを `/var/log` の場所に配置します。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）] タブをクリックします。

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 [ワーク（Work）]ペインで [コントローラ情報（Controller Info）] タブをクリックします。

ステップ 4 [アクション（Actions）]領域で、[TTY ログの取得（Get TTY Log）] 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。

重要 コントローラの TTY ログの取得には、最長で 2 ～ 4 分かかる場合があります。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 セキュリティの変更

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）]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 [ワーク（Work）]ペインで [コントローラ情報（Controller Info）] タブをクリックします。

ステップ 4 [アクション（Actions）]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。
[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が表示されます。

ステップ 5 [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、次の情報を確認します。

[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。
[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。

[名前（Name）]	説明
[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。

コントローラ セキュリティの無効化

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 [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 [ワーク（Work）]ペインで [コントローラ情報（Controller Info）] タブをクリックします。

ステップ 4 [アクション（Actions）]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。
プロンプトで [はい（Yes）]または [いいえ（No）] をクリックします。

コントローラ セキュリティの有効化

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 [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 [ワーク（Work）]ペインで [コントローラ情報（Controller Info）] タブをクリックします。

ステップ 4 [アクション（Actions）]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。
[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が表示されます。

ステップ 5 [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、次の情報を確認します。

表 *4*：*[*セキュア キー設定（*Secure Key Configuration*）*]* 領域

[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。
[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。

[名前（Name）]	説明
[候補（Suggest）]ボタン	使用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。

次の作業

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、適切な LSI MegaRAID コントローラが含まれている [サーバ 1（Server 1）] タブをクリックします。

ステップ 3 [ワーク（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、[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）]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 [ワーク（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、専用ホット スペアを作成する物理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	説明
[仮想ドライブ番号（Virtual Drive Number）]ドロップダウン リスト	物理ドライブをホット スペア専用に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。
[物理ドライブ番号（Physical Drive Number）]フィールド	物理ドライブの番号。

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）]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 [ワーク（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、グローバル ホット スペアを作成する物理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）] タブをクリックします。

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 [ワーク（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）]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 [ワーク（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、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、[状態を未設定良好に設定（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 に設定（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 に設定（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。
[状態を未設定良好に設定（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）] タブをクリックします。

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 [ワーク（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、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。

物理ドライブのフル ディスク暗号化の有効化

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。
- 物理ドライブは JBOD 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 [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 [ワーク（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、保護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、[フル ディスク暗号化の有効化（Enable Full Disk Encryption）] をクリックします。

セキュアな物理ドライブのクリア

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。
- 物理ドライブでフル ディスクの暗号化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 [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 [ワーク（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、保護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、[セキュア ドライブのクリア（Clear Secure Drive）] をクリックします。

セキュアな外部設定ドライブのクリア

外部設定をロックするために使用されるセキュリティ キーが失われると、データは取得できません。この場合は、HDD を廃棄するか、外部設定をクリアすることができます。

（注） 外部設定をクリアすると、ドライブからすべてのデータが消去されます。

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 [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 [ワーク（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、保護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、[セキュアな外部設定ドライブのクリア（Clear Secure Foreign Config Drive）] をクリックします。

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）] タブをクリックします。

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 [ワーク（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、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（FastInitialize）]：このオプションを使用すると、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。
- [完全初期化（FullInitialize）]：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	説明
[操作（Operation）]	ドライブで実行中の操作の名前。
[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）] タブをクリックします。

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 [ワーク（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、コントローラが起動に使用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）] タブをクリックします。

ステップ 2 [ストレージアダプタ（Storage Adapters）] タブの [LSI MegaRAID SAS 9266-8i] をクリックします。

ステップ 3 [ワーク（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 [アクション（Actions）]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ます。

ステップ 6 [移行する RAID レベルの選択（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 レベルの選択（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 に移行するには、RAID 0 に少なくとも 6 台のドライブが必要です。こ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 [仮想ドライブのプロパティ（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。

- [ライト スルー（WriteThrough）] : データはキャッシュ経由で物理ドライブに書き込まれます。該当データの以降の読み取りをキャッシュから行えるため、パフォーマンスが改善されます。
- [ライト バック（WriteBack）] : 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、[ライト スルー（Write Through）]キャッシングにフォールバックします。
- [不良 BBU のライト バック（WriteBack Bad BBU）] : このポリシーでは、バッテリ バックアップ ユニットに欠陥または放電があった場合も、書き込みキャッシングは [ライト 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。

仮想ドライブの保護

仮想ドライブのフル ディスクの暗号化を有効にした後でのみ、そのドライブを保護できます。未使用の物理ドライブから仮想ドライブを作成するときにこの操作を実行できます。暗号化を行うのが物理ドライブであるため、ドライブ グループ内の仮想ドライブが 1 台保護されると、ドライブ グループ内のすべての仮想ドライブが保護されます。仮想ドライブはドライブ グループのセキュリティ設定を継承します。

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。
- 仮想ドライブでフル ディスクの暗号化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 [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 [ワーク（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、保護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、[仮想ドライブの保護（Secure Virtual Drive）] 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、保持する必要があるデータをバック アップしてください。

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）]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 [ワーク（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、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。

バッテリバックアップユニットの自動学習サイクルのイネーブル化

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）]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 [ワーク（Work）]ペインで [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 [自動学習モードの有効化（Enable Auto Learn Mode）] 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。

バッテリ バックアップ ユニットの自動学習サイクルのディセーブル化

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）]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 [ワーク（Work）]ペインで [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 [自動学習モードの無効化（Disable Auto Learn Mode）] 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。

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）] タブをクリックします。

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 [ワーク（Work）]ペインで [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。

物理ドライブのロケータ LED の切り替え

はじめる前に

このタスクを実行するには、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）]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 [ワーク（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 [ステータス（Status）]領域で、[ロケータ LED（Locator LED）] フィールドの [オンにする（Turn On）] または [オフにする（Turn Off）] オプション ボタンを選択します。

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）] タブをクリックします。

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 [ワーク（Work）]ペインの [ストレージ ログ（Storage Log）] タブをクリックし、次の情報を確認します。

[名前（Name）]	説明
[時間（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 • 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することができます。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）]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 [ワーク（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
[電源再投入カウント（Power Cycle Count）] フィールド	ドライブが製造されてから電源の再投入が行われた回数。
[電源投入時間（Power on Hours）]フィールド	ドライブが「電源オン」モードになっている合計時間数。

[名前（Name）]	説明
[ライフ残存率（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、ライフタイム中に 100 の書き込みサイクルが可能な SSD で、15 の書き込みが完了している場合、ドライブに残っているライフのパーセンテージは 85 % です。
[劣化ステータス（日）（Wear Status in Days）]フィールド	SSD で書き込みサイクルが行われた日数。 SSD ベンダーによって、SSD での 1 日の書き込み上限数が指定されています。これを基に SSD が動作を継続可能な合計年数を計算できます。
[動作温度（Operating Temperature）]フィールド	特定の時刻に選択した SSD が動作するドライブの現在の温度。

第 11 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）] タブをクリックします。

ステップ 2 [管理者（Admin）] タブの [コミュニケーション サービス（Communications 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 [コミュニケーション サービス（Communication Services）] タブをクリックします。

ステップ 4 [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 の有効化（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 を HTTPS にリダイレクトの有効化（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 要求の間に、Cisco IMCがタイムアウトしてセッションが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 5 [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）] タブをクリックします。

ステップ 2 [管理者（Admin）] タブの [コミュニケーション サービス（Communications 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 [コミュニケーション サービス（Communication Services）] タブをクリックします。

ステップ 4 [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 の有効化（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 5 [変更の保存（Save Changes）]をクリックします。

XML API の設定

Cisco IMCの XML API

Cisco Cisco IMCXML 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）] タブをクリックします。

ステップ 2 [管理者（Admin）] タブの [コミュニケーション サービス（Communications 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 [コミュニケーション サービス（Communication Services）] タブをクリックします。

ステップ 4 [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 の有効化（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 5 [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）] タブをクリックします。

ステップ 2 [管理者（Admin）] タブの [コミュニケーション サービス（Communications 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 [コミュニケーション サービス（Communication Services）] タブをクリックします。

ステップ 4 [IPMI over LAN プロパティ（IPMI 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	このサーバで IPMI アクセスが許可されているかどうか。

[名前（Name）]	説明
[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、それ以外に所持している IPMI 特権に関係なく、読み取り専用の IPMI セッションだけです。 • [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 暗号キーをランダムな値に変更できます。

ステップ 5 [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およびアラート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）] タブをクリックします。

ステップ 2 [管理者（Admin）] タブの [コミュニケーション サービス（Communications 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 の有効化（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、[変更の保存（Save Changes）]をクリックする必要があります。
[SNMP ポート（SNMP Port）] フィールド	Cisco IMCSNMP 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。

[名前（Name）]	説明
[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への部分的な読み取りアクセスを提供します。 • [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 コンタクト（System Contact）]フィールド	SNMP の実装を担当するシステムの連絡先責任者。 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）が稼働するホストの場所。 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。
[SNMP エンジン ID（SNMP Engine ID）]フィールド	管理用に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、その値からこの文字列が生成されます。定義されていない場合は、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 トラップの設定, （273 ページ）の説明に従って SNMP トラップを設定します。

SNMP トラップの設定

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 [コミュニケーション サービス（Communications 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、[変更（Modify）]をクリックします。
- [追加（Add）]をクリックして新しいユーザを作成します。

（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	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。
[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	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。 • [通知（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。

[名前（Name）]	説明
[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の宛先の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、行を選択して [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）] タブをクリックします。

ステップ 2 [管理者（Admin）] タブの [コミュニケーション サービス（Communications Services）] をクリックします。

ステップ 3 [SNMP]タブをクリックし、[トラップ宛先（Trap Destinations）] タブをクリックします。

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には、トラップが設定済みで、イネーブルになっている必要があります。

SNMPv3 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）] タブをクリックします。

ステップ 2 [管理者（Admin）] タブの [コミュニケーション サービス（Communications 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 [SNMPv3 ユーザ（SNMPV3 Users）]領域で、次のプロパティを更新します。

[名前（Name）]	説明
[追加（Add）] 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。
[変更（Modify）] 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。
[削除（Delete）] 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）]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。

SNMPv3 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）] タブをクリックします。

ステップ 2 [管理者（Admin）] タブの [コミュニケーション サービス（Communications 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（Users）]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、[変更（Modify）]をクリックします。
- [ユーザ（Users）]領域で行を選択し、[追加（Add）] 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	ユーザの固有識別子。このフィールドは変更できません。
[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。

[名前（Name）]	説明
[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。 • [認証なし、プライバシーなし（noauth, no priv）]：このユーザには、認証パスワードもプライバシー パスワードも不要です。 • [認証あり、プライバシーなし（auth, no priv）]：このユーザには、認証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、後述の認証フィールドが Cisco IMCによって有効になります。 • [認証、プライバシー（auth, priv）]：このユーザには、認証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によって認証およびプライバシーのフィールドが有効になります。
[認証タイプ（Auth Type）]ドロップダウン	認証タイプ。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 ユーザの認証パスワード。 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	確認のために認証パスワードを再入力します。
[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。
[プライバシー パスワードの確認（Confirm Privacy Password）]フィールド	確認のために認証パスワードを再入力します。

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、ユーザを選択して [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。

第 12 章

証明書の管理

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さは 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） アップロードされた証明書は、Cisco IMCによって生成された CSR から作成されている必要があります。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）] フィールドでは、特殊文字（アンパサンド（**&**）など）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）] タブをクリックします。

ステップ 2 [管理者（Admin）] タブの [証明書管理（Certificate Management）] をクリックします。

ステップ 3 [アクション（Actions）]領域で、[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きに、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。
[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。
[都道府県（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都道府県。
[国コード（Country Code）]ドロップダウン リスト	会社が存在する国。
[メール（Email）]フィールド	会社の電子メールの連絡先。
[自己署名証明書（Self Signed Certificate）]チェックボックス	自己署名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）** イネーブルにすると、自動的に CSR が生成され、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 を開いています（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) [開く（Open With）]をクリックして csr.txt を表示します。

b) [ファイルの保存（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。

信頼できない CA 署名付き証明書の作成

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_keyfilenamekeysize* 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。

	コマンドまたはアクション	目的
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。
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 **Server SSL** および **Netscape SSL** サーバの値が 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。

	コマンドまたはアクション	目的
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

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） 最初にCisco IMCの [証明書の管理（Certificate Management）] メニューを使用して 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）] タブをクリックします。

ステップ 2 [管理者（Admin）] タブの [証明書管理（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	目的の証明書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。
[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。

サーバ証明書の内容の貼り付け

ローカル ファイル システムからサーバ証明書をアップロードする代わりに、テキスト フィールドに証明書の内容を貼り付けることで新しいサーバ証明書をアップロードすることもできます。

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。
- アップロードする証明書が署名されていることを確認します。

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）] タブの [証明書管理（Certificate Management）] をクリックします。

ステップ 3 [アクション（Actions）]領域で [サーバ証明書の貼り付け（Paste Server Certificate）] をクリックします。

[サーバ証明書の貼り付け（Paste Server Certificate）]ダイアログボックスが表示されます。

ステップ 4 [サーバ証明書の貼り付け（Paste Server Certificate）]ダイアログ ボックスで、[証明書（Certificate）] テキスト フィールドにサーバ証明書の内容を貼り付け、[保存（Save）] をクリックします。
これにより、サーバに証明書がアップロードされます。

新しい証明書のトラブルシューティング

場合によっては、新しい証明書がシステムに表示されないことがあります。その場合、次のトラブルシューティング手順を実行し、Cisco IMC をリブートする必要があります。

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。
- 新しい証明書をアップロード済みである必要があります。

手順

ステップ 1 Cisco IMC サーバで新しいセキュア シェル セッションを開始します。

ステップ 2 **scope certificate** および **show detail** コマンドをそれぞれ実行し、アップロードした証明書が表示されることを確認します。

ステップ 3 セキュア シェルのコマンドライン インターフェイスを終了します。

ステップ 4 Cisco IMC Web インターフェイスにログインします。

ステップ 5 [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 6 [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 7 [ユーティリティ（Utilities）]ペインの [アクション（Actions）] 領域で、[Cisco IMC の再起動（Reboot Cisco IMC）] をクリックします。

ステップ 8 [OK]をクリックします。

ステップ 9 Web ブラウザの履歴をクリアします。

ステップ 10 Cisco IMC からログアウトしてから再度ログインし、新しい証明書が使用されていることを確認します。

第 13 章

プラットフォームイベントフィルタの設定

この章の内容は、次のとおりです。

プラットフォーム イベント フィルタ

プラットフォーム イベント フィルタ（PEF）は、アクションをトリガーできます。PEF ごとに、プラットフォーム イベントが発生したときに実行するアクション（またはアクションを実行しないこと）を選択できます。

プラットフォーム イベント フィルタの設定

はじめる前に

プラットフォーム イベント フィルタを設定するには、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）] タブをクリックします。

ステップ 2 [管理者（Admin）] タブの [イベント管理（Event Management）] をクリックします。

ステップ 3 [プラットフォーム イベント フィルタ（Platform Event Filters）]領域で、各イベントの次のフィールドに入力します。

[名前（Name）]	説明
[ID]カラム	一意のフィルタ ID。
[イベント（Event）]カラム	イベント フィルタの名前。
[アクション（Action）]カラム	フィルタごとに、目的の処理をスクロール リスト ボックスから選択します。次のいずれかになります。 • [なし（None）] : アクションは実行されません。 • [再起動（Reboot）] : サーバがリブートされます。 • [電源再投入（PowerCycle）] : サーバの電源が再投入されます。 • [電源オフ（PowerOff）] : サーバの電源がオフになります。

ステップ 4 [変更の保存（Save Changes）]をクリックします。

プラットフォーム イベント フィルタのリセット

手順

ステップ 1 [ナビゲーション（Navigation）]ペインの [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 [イベント管理（Event Management）] をクリックします。

ステップ 3 [プラットフォーム イベント フィルタ（Platform Event Filters）]領域で、[イベント フィルタのリセット（Reset Event Filters）] をクリックします。
イベント フィルタがリセットされ、最新のイベント フィルタが表示されます。

第 14 章

Cisco IMC ファームウェア管理

この章の内容は、次のとおりです。

ファームウェアの概要

C シリーズ サーバは、使用する C シリーズ サーバ モデルに特有のシスコ認定ファームウェアを使用します。すべてのサポート対象サーバモデルのファームウェアの新しいリリースは、Cisco.com からダウンロードできます。

注意 新しい BIOS ファームウェアをインストールするとき、それはサーバで実行されているCisco IMCファームウェアと同じソフトウェア リリースに属する必要があります。新しいBIOSファームウェアのインストールは、必ず一致する Cisco IMCファームウェアをアクティブにした後に行ってください。そうしないと、サーバはブートしません。

起こりうる問題を避けるため、Cisco Host Upgrade Utility（HUU）を使用することを強く推奨します。このユーティリティはBIOS、Cisco IMC、およびその他のファームウェアを互換性のあるレベルにアップグレードします。このユーティリティの詳細については、インストールするCisco IMCソフトウェア リリースに対応する HUU のバージョンの『『*Cisco Host Upgrade Utility Guide*』』を参照してください。HUU ガイドは次の URL で入手できます。http://www.cisco.com/en/US/products/ps10493/products_user_guide_list.html。

ファームウェアを手動で更新する場合は、最初にCisco IMCファームウェアを更新する必要があります。Cisco IMCファームウェアの更新プロセスは、次の段階に分けられます。これは、サーバがオフラインになる時間を最小限にするためです。

- インストール：この段階では、Cisco IMCは選択した Cisco IMC ファームウェアをサーバの非アクティブまたはバックアップのスロットにインストールします。
- アクティベーション：この段階では、Cisco IMCは非アクティブのファームウェア バージョンをアクティブとして設定するため、サービスの中断の原因となります。サーバをリブートすると、新規のアクティブ スロット内のファームウェアが、実行中のバージョンになります。

Cisco IMCファームウェアを有効化した後は、BIOS ファームウェアを更新できます。BIOS 更新のプロセス全体でサーバの電源をオフにする必要があるため、プロセスは段階に分類されません。その代わり、入力するコマンドは 1 つで済みます。Cisco IMCは BIOS ファームウェアをできる限り迅速にインストールし、更新します。Cisco IMCがリブートを完了すると、サーバの電源をオンにして、サービスに戻すことができます。

（注）
- 古いファームウェア バージョンを新しいものにアップグレードしたり、新しいファームウェア バージョンを古いものにダウングレードしたりできます。
- この手順は、スタンドアロン モードで実行している Cisco UCS C シリーズ サーバにのみ適用されます。Cisco UCS Manager の統合モードで実行している UCS C シリーズのファームウェアをアップグレードするには、Cisco Technical Assistance Center にお問い合わせください。

セキュア モードの Cisco IMC では、ロードおよび実行前のすべてのファームウェア イメージがデジタル的に署名され、信頼性と整合性が確認され、改竄されたソフトウェアの実行からデバイスを確実に保護できます。

シスコからのファームウェアの入手

手順

ステップ 1 http://www.cisco.com/ にアクセスします。

ステップ 2 まだログインしていない場合は、ページの右上隅にある [ログイン（Log In）] をクリックし、Cisco.com のクレデンシャルを使用してログインします。

ステップ 3 上部のメニュー バーで、[サポート（Support）] をクリックします。

ステップ 4 ロール ダウン メニューの [すべてのダウンロード（All Downloads）] をクリックします。

ステップ 5 使用しているサーバ モデルが [最近使用した製品（Recently Used Products）]リストに表示される場合は、サーバ名をクリックします。含まれていない場合は、次の手順を実行します。

a) 左側のボックスの [製品（Products）] をクリックします。

b) 中央のボックスで、[ユニファイド コンピューティングおよびサーバ（Unified Computing and Servers）]をクリックします。

c) 右側のボックスで、[Cisco UCS C-Series ラックマウント スタンドアロン サーバ ソフトウェア（Cisco UCS C-Series Rack-Mount Standalone Server Software）] をクリックします。

d) 右のボックスで、ソフトウェアをダウンロードするサーバ モデルをクリックします。

ステップ 6 [ユニファイド コンピューティング システム（UCS）サーバ ファームウェア（Unified Computing System (UCS) Server Firmware）] リンクをクリックします。

ステップ 7 （任意） ページに左側にあるメニュー バーから以前のリリースを選択します。

ステップ 8 選択したリリースの Cisco Host Upgrade Utility ISO に関連付けられている [ダウンロード（Download）] ボタンをクリックします。

ステップ 9 [使用許諾契約に同意] をクリックします。

ステップ 10 ISO ファイルをローカル ドライブに保存します。
この ISO ファイルを使用してサーバの Cisco IMC と BIOS ファームウェアをアップグレードすることをお勧めします。この ISO ファイルには、Cisco Host Upgrade Utility が含まれます。このユーティリティの詳細については、インストールする Cisco IMC ソフトウェア リリースに対応する HUU のバージョンの『『*Cisco Host Upgrade Utility Guide*』』を参照してください。HUU ガイドは次の URL で入手できます。http://www.cisco.com/en/US/products/ps10493/products_user_guide_list.html。

ステップ 11 （任意） Cisco IMC と BIOS ファームウェアを手動でアップグレードする予定の場合、次の手順を実行します。

a) ISO ファイルから、ファームウェア インストール ファイルを含む ZIP ファイルを開きます。この ZIP ファイルは ISO ファイルの最上位レベルにあり、ファイル名の書式は `ServerModel_ReleaseNumber.ZIP` に従います。

たとえば、`C240M3_1.4.4A.ZIP` などです。

この ZIP ファイルに含まれるすべてのファイルを抽出する必要はありません。このファイルを開くだけで、BIOS ファームウェアのインストール用 CAP ファイルと、Cisco IMC ファームウェアのインストール用 BIN ファイルが含まれる ZIP ファイルにアクセスできます。

b) *ServerModel_ReleaseNumber*.ZIP ファイルから BIOS ファームウェア インストール CAP ファイルを抽出して、ローカル ドライブに保存します。
CAP ファイルは *ReleaseNumber*/bios/cisco imc フォルダにあり、ファイル名は *Server*-BIOS-*Release-Number*.CAP という形式です。

たとえば、1.4.4a/bios/cisco imc/C240-BIOS-1-4-4c-0.CAP などです。

c) *ServerModel_ReleaseNumber*.ZIP ファイルから、Cisco IMC ファームウェアのインストール用ファイルを含む ZIP ファイルを開きます。
ZIP ファイルは *ReleaseNumber*/cisco imc フォルダにあり、ファイル名は *server-model*-cisco imc-*release*.zip という形式です。

たとえば、1.4.4a/cisco imc/c240-m3-cisco imc.1.4.4a.zip などです。

この zip ファイルに含まれるすべてのファイルを抽出する必要はありません。このファイルを開くだけで、Cisco IMCファームウェアのインストール用 BIN ファイルにアクセスできます。

d) *server-model*-cisco imc-*release*.zip ファイルから、完全な Cisco IMC ファームウェアのインストール用 BIN ファイルを抽出し、ローカル ドライブに保存します。
BIN ファイルは *server-model*-cisco imc-*release* フォルダにあり、ファイル名は upd-pkg-*server-model*-cisco imc.full.*release*.bin という形式です。

たとえば、c240-m3-cisco imc.1.4.4a/upd-pkg-c240-m3-cisco imc.full.1.4.4a.bin などです。

ステップ 12 （任意） リモート サーバからファームウェアをインストールする予定の場合、そのリモート サーバに BIOS のインストール用 CAP ファイルと Cisco IMCインストール用 BIN ファイルをコピーします。
リモート サーバは次のいずれかになります。

- TFTP
- FTP
- SFTP
- SCP
- HTTP

サーバにはリモート サーバのコピー先フォルダに対する読み取り権限が必要です。

（注） Cisco UCS C シリーズ サーバでは、リモート サーバからファームウェアを更新した場合のサーバのフィンガープリントの確認がサポートされるようになりました。このオプションは、リモート サーバ タイプとして SCP または SFTP を選択した場合にのみ使用できます。

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、「Server (RSA) key fingerprint is <server_finger_print _ID> Do you wish to continue?」というメッセージが表示されます。サーバ フィンガープリントの信頼性に応じて、[Y] または [N] 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。

次の作業

Cisco Host Upgrade Utility を使用してサーバ上のすべてのファームウェアをアップグレードするか、手動でサーバに Cisco IMC ファームウェアをインストールします。

Cisco IMC セキュア ブートについて

Cisco IMC のセキュア モードについて

（注） Cisco IMC のセキュア ブート モードは、一部の Cisco UCS C シリーズ サーバでのみデフォルトで有効になっています。

Host Upgrade Utility（HUU）、Web UI または CLI を使用して、Cisco IMC を最新バージョンに更新できます。Cisco IMC のアップグレードに HUU を使用する場合は、セキュア ブート モードを有効にするよう求めるプロンプトが表示されます。[はい（Yes）]を選択すると、セキュア モードが開始され、ファームウェアが 2 度インストールされます。[いいえ（No）]を選択すると、非セキュア モードが開始されます。Cisco IMC をアップグレードするために Web UI または CLI を使用する場合は、バージョン 2.0(x) にアップグレードする必要があります。バージョン 2.0(x) でシステムを起動した後、システムはデフォルトでは非セキュア モードで起動します。セキュア モードを有効にする必要があります。セキュア モードを有効にすると、自動的にファームウェアが再インストールされます。Web UI では、セキュア モード オプションが Cisco IMC ファームウェア更新ページ内のチェックボックスとして利用できます。CLI では、**update-secure** コマンドを使用してセキュア モードを有効にできます。

Cisco IMC バージョン 2.0 への最初のアップグレード時に、機能およびアプリケーションの一部が正しくインストールされておらず、2 回目のアップグレードが必要であることを示す警告メッセージが表示される場合があります。セキュア ブート オプションが有効か無効かにかかわらず、Cisco IMC ファームウェア バージョン 2.0(x) をセキュア モードで正しくインストールするために、2 回目のアップグレードを実行することを推奨します。インストールが完了した後、イメージをアクティブ化する必要があります。セキュア ブート オプションを有効にしてシステムを起動した後は、Cisco IMC がセキュア モードのままとなり、後でこれを無効にすることはできません。イメージをアクティブ化せずに他のファームウェア イメージを再インストールすると、Cisco IMC が応答不能になる場合があります。

警告 セキュア ブートの移行でファームウェアをインストールした後は、他の通常のサーバベースのタスクを実行する前にイメージをアクティブ化する必要があります。このイメージをアクティブ化せずに他のファームウェア イメージを再インストールすると、Cisco IMC が応答不能になる場合があります。

セキュア ブートは、ファームウェアのインストールが完了し、イメージをアクティブ化した場合にのみ有効になります。

（注） Cisco IMC がセキュア モードになっている場合、次のことを意味します。

- デバイスにインストールして起動できるのは、署名済みの Cisco IMC ファームウェア イメージのみです。
- セキュア Cisco IMC モードを後で無効にすることはできません。
- いずれの Cisco IMC バージョンも最新バージョンに直接アップグレードできます。
- バージョン 1.5(3x) より前の Cisco IMC ファームウェア バージョンは、インストールまたは起動できません。
- Cisco IMC バージョン 2.0 は、バージョン 1.4(x)、1.5、1.5(2x)、または 1.5(1)、1.5(2) または非セキュアのファームウェア バージョンにダウングレードできません。

最新バージョンからダウングレードする際にサポートされる Cisco IMC バージョン

次の表は、前のバージョンにダウングレードできるセキュア モードの Cisco IMC バージョンを示します。

元の Cisco IMC バージョン	目的の Cisco IMC バージョン	可/不可
2.0(x)	1.5(1) よりも前	不可
2.0(x)	1.5(3x) 以降	最大獲得ポイント（Possible）
2.0(x)	1.5(3x) よりも前	不可

（注） 使用している Cisco IMC のバージョンが非セキュア モードの場合、Cisco IMC を以前のバージョンにダウングレードすることができます。

（注） HUU を使用して 1.5(4) より前のバージョンに Cisco IMC バージョンをダウングレードする場合は、最初に Cisco IMC をダウングレードし、その後に他のファームウェアをダウングレードする必要があります。ファームウェアをアクティブにし、次に BIOS ファームウェアをダウングレードします。

Cisco IMC バージョン 2.0(1) に必要な更新回数

重要 この項は、Cisco IMC バージョン 2.0(1) 以前のリリースに有効です。

最新バージョンにアップグレードする際にサポートされる Cisco IMC バージョン

次の表に、最新バージョンのすべてのアプリケーションを正しくインストールするために Cisco IMC に必要な更新回数を示します。

元の Cisco IMC バージョン	非セキュア Cisco IMC バージョン 2.0(x) へ	セキュア Cisco IMC バージョン 2.0(x) へ
1.5(2) よりも前	更新 2 回	更新 2 回
1.5(2)	更新 1 回	更新 2 回
1.5(3)	更新 1 回	更新 2 回
1.5(3x) 以降	更新 1 回	更新 2 回

非セキュア モードでの Cisco IMC の更新

重要 この項は、Cisco IMC バージョン 2.0(1) 以前のリリースに有効です。

すべての最新機能とアプリケーションが正常にインストールされた状態で、非セキュア モードで Cisco IMC を最新バージョンにアップグレードできます。Web UI または CLI を使用して Cisco IMC を最新バージョンにアップグレードするときは、使用しているバージョンによってはファームウェアを手動で 2 回更新する必要があります。「最新バージョンにアップグレードする際にサポートされる Cisco IMC バージョン」を参照してください。HUU を使用して Cisco IMC バージョンをアップグレードすると、最新バージョンに自動的にアップグレードされます。

（注） 1.5(2x) よりも前のバージョンの Cisco IMC からインストールする場合は、次のメッセージが表示されます。

警告 「一部の Cisco IMC ファームウェア コンポーネントが正しくインストールされていません。Cisco IMC ファームウェア バージョン 2.0(1) 以降を再インストールして回復させてください。（Some of the Cisco IMC firmware components are not installed properly! Please reinstall Cisco IMC firmware version 2.0(1) or higher to recover.）」

（注） （HUUによる）更新の最中は、KVMセッションに再接続して更新の現在のステータスを取
することを推奨します。

Cisco IMC が非セキュア モードで実行している場合は、次を意味します。

- 署名済みまたは未署名の Cisco ファームウェア イメージをデバイスにインストールできます。
- いずれの Cisco IMC バージョンも最新バージョンに直接アップグレードできます。
- Cisco IMC のファームウェア バージョンは以前のバージョンにインストールまたは起動できます。

リモート サーバからの Cisco IMCファームウェアのインストール

はじめる前に

- admin 権限を持つユーザとして Cisco IMC GUI にログインします。
- Cisco.com から Cisco Host Upgrade Utility ISO ファイルを入手し、シスコからのファームウェアの入手, （293 ページ） の説明に従ってファームウェア インストール ファイルを抽出します。

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）] タブの [ファームウェア管理（Firmware Management）] をクリックします。

ステップ 3 [アクション（Actions）]領域で、[リモート サーバからの Cisco IMC ファームウェアのインストール（Install Cisco IMC Firmware from Remote Server）] をクリックします。

ステップ 4 [Cisco IMC ファームウェアのインストール（Install Cisco IMC Firmware）] 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
[Cisco IMC ファームウェアのインストール元（Install Cisco IMC Firmware 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）
[TFTP サーバ IP/ホスト名（TFTP Server IP/Hostname）]フィールド	Cisco IMC ファームウェア インストール ファイルが存在するサーバの IP アドレスまたはホスト名。[Cisco IMC ファームウェアのインストール元（Install Cisco IMC Firmware 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。
[イメージパスおよびファイル名（Image Path and Filename）]フィールド	リモート サーバ上の Cisco IMC ファームウェア インストール ファイルのパスおよびファイル名。

[名前（Name）]	説明
[ファームウェアのインストール（Install Firmware）] ボタン	最新のアップデートでCisco IMCファームウェアを再インストールします。Cisco IMCのセキュアブートがイネーブルの状態でファームウェアをインストールする場合は、ファームウェア イメージをアクティブにする必要があります。 （注） リモート サーバタイプとしてSCPまたはSFTPを選択してこのアクションを実行した場合、ポップアップ ウィンドウに「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。 （注） セキュアブートの移行でファームウェアをインストールした後は、他の通常のサーバベースのタスクを実行する前にイメージをアクティブ化する必要があります。このイメージをアクティブ化せずに他のファームウェア イメージを再インストールすると、Cisco IMC が応答不能になる場合があります。 セキュアブートは、ファームウェアのインストールが完了し、イメージをアクティブ化した場合にのみ有効になります。
[閉じる（Close）]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 5 [ファームウェアのインストール（Install Firmware）]をクリックします。

次の作業

Cisco IMCファームウェアをすぐにアクティブにします。

ブラウザ経由の Cisco IMC ファームウェアのインストール

はじめる前に

- admin 権限を持つユーザとして Cisco IMC GUI にログインします。
- Cisco.com から Cisco Host Upgrade Utility ISO ファイルを入手し、シスコからのファームウェアの入手, （293 ページ） の説明に従ってファームウェア インストール ファイルを抽出します。

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）] タブの [ファームウェア管理（Firmware Management）] をクリックします。

ステップ 3 [アクション（Actions）]領域で、[ブラウザ クライアント経由の Cisco IMC ファームウェアのインストール（Install Cisco IMC Firmware through Browser Client）] をクリックします。

ステップ 4 [ファームウェアのインストール（Install Firmware）]ダイアログボックスで、[参照（Browse）] をクリックし、[ファイルの選択（Choose File）] ダイアログボックスを使用してインストールする .bin ファイルを選択します。

ステップ 5 （任意） [Cisco IMC セキュア ブートを有効にする（Enable Cisco IMC Secure Boot）]チェックボックスをオンにして、Cisco IMC のセキュア モードをイネーブルにします。

（注） このオプションは Cisco IMC バージョン 2.0(1) でのみ使用できます。以降のバージョンでは、デフォルトで有効になっています。

オンにすると、セキュア ブートがイネーブルの場合は署名済みの Cisco IMC ファームウェア イメージのみをデバイスにインストールできることを示すメッセージが、確認ダイアログボックスに表示されます。また、未署名の Cisco IMC ファームウェア イメージまたは 1.5(3x) より前の Cisco IMC バージョンのイメージはサポートされません。セキュア ブートで Cisco IMC を続行する場合は、[OK]を選択します。セキュア ブートで Cisco IMC を続行しない場合は、[キャンセル（Cancel）]を選択します。

重要 セキュア ブートをイネーブルにすると、後でディセーブルにできません。また、Cisco IMC はセキュア モードで続行します。

ステップ 6 [ファームウェアのインストール（Install Firmware）]をクリックします。

（注） セキュア ブートの移行でファームウェアをインストールした後は、他の通常のサーバベースのタスクを実行する前にイメージをアクティブ化する必要があります。このイメージをアクティブ化せずに他のファームウェア イメージを再インストールすると、Cisco IMC が応答不能になる場合があります。

Cisco IMC バージョン 2.0(1) の場合、セキュア ブートは、ファームウェアのインストールが完了し、イメージがアクティブになっている場合にのみイネーブルになります。

次の作業

Cisco IMC ファームウェアをすぐにアクティブにします。

インストールされているCiscoIMCファームウェアの有効化

はじめる前に

Cisco IMCファームウェアをサーバにインストールします。

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。
- Cisco IMCのリブートまたはリセット。
- 他のファームウェアの有効化。
- テクニカル サポートまたは設定データのエクスポート。

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 [ファームウェア管理（Firmware Management）] をクリックします。

ステップ 3 [アクション]領域で、[CIMCファームウェアの有効化（Activate CIMC Firmware）][Cisco IMC ファームウェアの有効化（Activate Cisco IMC Firmware）] 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 4 [ファームウェアの有効化（Activate Firmware）] ダイアログボックスで、有効化するファームウェア イメージを選択します。

ステップ 5 [ファームウェアの有効化（Activate Firmware）] をクリックします。

リモートサーバからのBIOSファームウェアのインストール

（注） この手順は、一部のサーバでは使用できません。他の BIOS インストール方法については、次の URL で入手できる『『*Cisco UCS C-Series Rack-Mount Server BIOS Upgrade Guide*』』を参照してください。http://www.cisco.com/en/US/docs/unified_computing/ucs/c/sw/bios/b_Upgrading_BIOS_Firmware.html

はじめる前に

- admin 権限を持つユーザとして Cisco IMC GUI にログインします。
- インストールされている Cisco IMCファームウェアの有効化, （302 ページ）の説明に従って、インストールする BIOS バージョンに対応する Cisco IMC ファームウェアをアクティブにします。
- サーバの電源を切ります。

（注） C220 M4、C240 M4 および C3160 の場合は、サーバの電源をオフにする必要はありません。

注意 新しい BIOS ファームウェアをインストールするとき、それはサーバで実行されているCisco IMCファームウェアと同じソフトウェア リリースに属する必要があります。新しいBIOS ファームウェアのインストールは、必ず一致する Cisco IMCファームウェアをアクティブにした後に行ってください。そうしないと、サーバはブートしません。

起こりうる問題を避けるため、Cisco Host Upgrade Utility（HUU）を使用することを強く推奨します。このユーティリティはBIOS、Cisco IMC、およびその他のファームウェアを互換性のあるレベルにアップグレードします。このユーティリティの詳細については、インストールする Cisco IMCソフトウェア リリースに対応する HUU のバージョンの『『*Cisco Host Upgrade Utility Guide*』』を参照してください。HUU ガイドは次の URL で入手できます。http://www.cisco.com/en/US/products/ps10493/products_user_guide_list.html。

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 [サマリー（Summary）] をクリックします。

ステップ 3 [サーバのステータス（Server Status）]領域で、[電源の状態（Power State）]フィールドが [オフ（Off）] になっていることを確認します。[オン（On）] の場合は、[アクション（Actions）]領域

の [サーバの電源オフ（Power Off Server）] をクリックし、サーバの電源がオフになるまで待機してから続行します。

ステップ 4 [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 5 [管理者（Admin）] タブの [ファームウェア管理（Firmware Management）] をクリックします。

ステップ 6 [Cisco IMC ファームウェア（Cisco IMC Firmware）] 領域で、[稼働バージョン（Running Version）] フィールドに表示されるファームウェア バージョンが、インストールする BIOS ファームウェア バージョンと一致していることを確認します。

重要 Cisco IMCファームウェア バージョンが一致しない場合は、この手順を続行する前にCisco IMCファームウェアを有効化します。そうしないとサーバがブートしません。詳細については、インストールされている Cisco IMCファームウェアの有効化,（302ページ）を参照してください。

ステップ 7 [アクション（Actions）]領域で、[リモート サーバからの BIOS ファームウェアのインストール（Install BIOS Firmware from Remote Server）] をクリックします。

ステップ 8 [BIOS ファームウェアのインストール（Install BIOS Firmware）]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
[BIOS ファームウェアのインストール元（Install BIOS Firmware 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） リモート サーバ タイプとして SCP または SFTP を選択してこのアクションを実行した場合、ポップアップ ウィンドウに「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	BIOS ファームウェア インストール ファイルが存在するサーバの IP アドレスまたはホスト名。[BIOS ファームウェアのインストール元（Install BIOS Firmware from）] ドロップダウン リストの設定によって、フィールド名は異なる場合があります。

[名前（Name）]	説明
[イメージパスおよびファイル名（Image Path and Filename）]フィールド	リモート サーバ上の BIOS ファームウェア インストール 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 9 [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 10 ステータスが [完了（Completed Successfully）] に変わるまで、[前回の BIOS ファームウェア インストール（Last BIOS Firmware Install）]領域で [ステータス（Status）] フィールドのメッセージを確認します。

ステップ 11 サーバの電源を投入して、BIOS のアップグレードを完了します。

ブラウザ経由の BIOS ファームウェアのインストール

（注） この手順は、一部のサーバでは使用できません。他の BIOS インストール方法については、次の URL で入手できる『『*Cisco UCS C-Series Rack-Mount Server BIOS Upgrade Guide*』』を参照してください。http://www.cisco.com/en/US/docs/unified_computing/ucs/c/sw/bios/b_Upgrading_BIOS_Firmware.html

はじめる前に

- admin 権限を持つユーザとして Cisco IMC GUI にログインします。
- インストールされている Cisco IMCファームウェアの有効化, （302 ページ）の説明に従って、インストールする BIOS バージョンに対応する Cisco IMC ファームウェアをアクティブにします。
- サーバの電源を切ります。

（注） C220 M4、C240 M4 および C3160 の場合は、サーバの電源をオフにする必要はありません。

⚠

注意 新しい BIOS ファームウェアをインストールするとき、それはサーバで実行されているCisco IMCファームウェアと同じソフトウェア リリースに属する必要があります。新しいBIOSファームウェアのインストールは、必ず一致する Cisco IMCファームウェアをアクティブにした後に行ってください。そうしないと、サーバはブートしません。

起こりうる問題を避けるため、Cisco Host Upgrade Utility（HUU）を使用することを強く推奨します。このユーティリティはBIOS、Cisco IMC、およびその他のファームウェアを互換性のあるレベルにアップグレードします。このユーティリティの詳細については、インストールするCisco IMCソフトウェア リリースに対応する HUU のバージョンの『『*Cisco Host Upgrade Utility Guide*』』を参照してください。HUU ガイドは次の URL で入手できます。http://www.cisco.com/en/US/products/ps10493/products_user_guide_list.html。

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 [サマリー（Summary）] をクリックします。

ステップ 3 [サーバのステータス（Server Status）]領域で、[電源の状態（Power State）]フィールドが [オフ（Off）] になっていることを確認します。[オン（On）] の場合は、[アクション（Actions）]領域の [サーバの電源オフ（Power Off Server）] をクリックし、サーバの電源がオフになるまで待機してから続行します。

ステップ 4 [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 5 [管理者（Admin）] タブの [ファームウェア管理（Firmware Management）] をクリックします。

ステップ 6 [Cisco IMC ファームウェア（Cisco IMC Firmware）] 領域で、[稼働バージョン（Running Version）] フィールドに表示されるファームウェア バージョンが、インストールする BIOS ファームウェア バージョンと一致していることを確認します。

重要 Cisco IMCファームウェア バージョンが一致しない場合は、この手順を続行する前にCisco IMC ファームウェアを有効化します。そうしないとサーバがブートしません。詳細については、インストールされている Cisco IMCファームウェアの有効化, （302 ページ）を参照してください。

ステップ 7 [アクション（Actions）]領域で、[ブラウザ クライアント経由の BIOS ファームウェアのインストール（Install BIOS Firmware through Browser Client）] をクリックします。

ステップ 8 [BIOS ファームウェアのインストール（Install BIOS Firmware）]ダイアログボックスで、[参照（Browse）] をクリックし、[ファイルの選択（Choose File）] ダイアログボックスを使用して、インストールする CAP ファイルを選択します。

ステップ 9 [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 10 ステータスが [完了（Completed Successfully）] に変わるまで、[前回の BIOS ファームウェア インストール（Last BIOS Firmware Install）]領域で [ステータス（Status）] フィールドのメッセージを確認します。

ステップ 11 サーバの電源を投入して、BIOS のアップグレードを完了します。

インストールした BIOS ファームウェアの有効化

（注） [BIOS ファームウェアの有効化（Activate BIOS Firmware）]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。このオプションがないサーバでは、サーバを再起動することでインストールされている BIOS ファームウェアをアクティブにできます。

はじめる前に

- BIOS ファームウェアをサーバにインストールします。
- ホストの電源を切ります。

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。
- Cisco IMCのリブートまたはリセット。
- 他のファームウェアの有効化。
- テクニカル サポートまたは設定データのエクスポート。

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 [ファームウェア管理（Firmware Management）] をクリックします。

ステップ 3 [アクション（Actions）]領域で [BIOS ファームウェアの有効化（Activate BIOS Firmware）] 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 4 [ファームウェアの有効化（Activate Firmware）] ダイアログボックスで、有効化するファームウェア イメージを選択します。

ステップ 5 [ファームウェアの有効化（Activate Firmware）] をクリックします。

ブラウザ経由の CMC ファームウェアのインストール

はじめる前に

（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。

- admin 権限を持つユーザとして Cisco IMC GUI にログインします。
- Cisco.com から Cisco Host Upgrade Utility ISO ファイルを入手し、シスコからのファームウェアの入手, （293 ページ） の説明に従ってファームウェア インストール ファイルを抽出します。

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）] タブの [ファームウェア管理（Firmware Management）] をクリックします。

ステップ 3 [アクション（Actions）]領域で、[ブラウザクライアント経由のCMCファームウェアのインストール（Install CMC Firmware through Browser Client）] をクリックします。

ステップ 4 [ファームウェアのインストール（Install Firmware）]ダイアログボックスで、[参照（Browse）] をクリックし、[ファイルの選択（Choose File）] ダイアログボックスを使用してインストールする .bin ファイルを選択します。

ステップ 5 [CMC] ドロップダウン メニューから、[CMC-1] または [CMC-2] を選択します。

ステップ 6 [ファームウェアのインストール（Install Firmware）]をクリックします。

次の作業

CMC ファームウェアをすぐにアクティブにします。

リモートサーバからのCMCファームウェアのインストール

はじめる前に

- admin 権限を持つユーザとして Cisco IMC GUI にログインします。
- Cisco.com から Cisco Host Upgrade Utility ISO ファイルを入手し、シスコからのファームウェアの入手, （293 ページ） の説明に従ってファームウェア インストール ファイルを抽出します。

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）] タブの [ファームウェア管理（Firmware Management）] をクリックします。

ステップ 3 [アクション（Actions）]領域で、[リモート サーバからの CMC ファームウェアのインストール（Install CMC Firmware from Remote Server）] をクリックします。

ステップ 4 [CMC ファームウェアのインストール（Install CMC Firmware）]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
[CMC] ドロップダウン リスト	SIOC コントローラ 1 または 2 の CMC を選択できます。次のいずれかになります。 • CMC-1 • CMC-2
[CMC ファームウェアのインストール元（Install CMC Firmware 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） リモート サーバ タイプとして SCP または SFTP を選択してこのアクションを実行した場合、ポップアップ ウィンドウに「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。
[TFTP サーバ IP/ホスト名（TFTP Server IP/Hostname）]フィールド	CMC ファームウェア インストール ファイルが存在するサーバの IP アドレスまたはホスト名。[CMC ファームウェアのインストール元（Install CMC Firmware from）]ドロップダウン リストの設定によって、フィールド名は異なる場合があります。

[名前（Name）]	説明
[イメージパスおよびファイル名（Image Path and Filename）]フィールド	リモート サーバ上の CMC ファームウェア インストール 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。
[ファームウェアのインストール（Install Firmware）]ボタン	最新のアップデートでCMCファームウェアを再インストールします。
[閉じる（Close）]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 5 [ファームウェアのインストール（Install Firmware）]をクリックします。

次の作業

CMC ファームウェアをすぐにアクティブにします。

インストールした CMC ファームウェアの有効化

はじめる前に

CMC ファームウェアをサーバにインストールします。

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。
- Cisco IMCのリブートまたはリセット。
- 他のファームウェアの有効化。
- テクニカル サポートまたは設定データのエクスポート。

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 [ファームウェア管理（Firmware Management）] をクリックします。

ステップ 3 [アクション（Actions）]領域で [CMC ファームウェアの有効化（Activate CMC Firmware）] 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 4 [ファームウェアの有効化（Activate Firmware）] ダイアログボックスで、有効化するファームウェア イメージを選択します。

ステップ 5 [ファームウェアの有効化（Activate Firmware）] をクリックします。

ブラウザ経由の SAS エクスパンダ ファームウェアのインストール

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。
- サーバの電源をオンにします。

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）] タブの [ファームウェア管理（Firmware Management）] をクリックします。

ステップ 3 [アクション（Actions）]領域で、[ブラウザ クライアント経由の SAS エクスパンダ ファームウェアのインストール（Install SAS Expander Firmware through Browser Client）] をクリックします。

ステップ 4 [SAS エクスパンダ ファームウェアのインストール（Install SAS Expander Firmware）]ダイアログボックスで[ファイルの選択（Choose File）] ボタンをクリックし、インストールするファームウェア イメージを選択します。

ステップ 5 [SAS エクスパンダ（SAS Expander）] ドロップダウン リストから SAS エクスパンダを選択します。

ステップ 6 [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 7 サーバの電源を投入して、アップグレードを完了します。

リモート サーバ経由の SAS エクスパンダ ファームウェアのインストール

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。
- サーバの電源をオンにします。

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）] タブの [ファームウェア管理（Firmware Management）] をクリックします。

ステップ 3 [アクション（Actions）]領域で、[リモート サーバからの SAS エクスパンダ ファームウェアのインストール（Install SAS Expander Firmware from Remote Server）] をクリックします。

ステップ 4 [SAS エクスパンダ ファームウェアのインストール（Install SAS Expander Firmware）]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
[SAS エクスパンダ（SAS Expander）]ドロップダウンリスト	ファームウェアをインストールする SAS エクスパンダを選択できます。 （注） 一部のサーバでは、SAS エクスパンダを 1 つのみ使用できます。

[名前（Name）]	説明
[SAS エクスパンダ ファームウェアのインストール元（Install SAS Expander Firmware 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） リモート サーバ タイプとして SCP または SFTP を選択してこのアクションを実行した場合、ポップアップ ウィンドウに「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	SAS エクスパンダ ファームウェア インストール ファイルが存在するサーバの IP アドレスまたはホスト名。[SAS エクスパンダ ファームウェアのインストール元（Install SAS Expander Firmware 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。
[イメージ パスおよびファイル名（Image Path and Filename）]フィールド	リモート サーバ上の SAS エクスパンダ ファームウェア インストール 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 [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 サーバの電源を投入して、アップグレードを完了します。

SAS エクスパンダ ファームウェアの有効化

はじめる前に

- SAS エクスパンダ ファームウェアをサーバにインストールします。
- ホストの電源をオンにします。

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。
- Cisco IMCのリブートまたはリセット。
- 他のファームウェアの有効化。
- テクニカル サポートまたは設定データのエクスポート。

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 [ファームウェア管理（Firmware Management）] をクリックします。

ステップ 3 [アクション（Actions）]領域で [SAS エクスパンダ ファームウェアの有効化（Activate SAS Expander Firmware）] をクリックします。
[SAS エクスパンダ ファームウェアの有効化（Activate SAS Expander Firmware）]ダイアログボックスが表示されます。

ステップ 4 [SAS エクスパンダ ファームウェアの有効化（Activate SAS Expander Firmware）]ダイアログボックスで、[SAS エクスパンダ（SAS Expander）] ドロップダウン リストからエクスパンダを選択します。

ステップ 5 オプション ボタンから SAS エクスパンダ ファームウェアのバージョンを選択します。

ステップ 6 [ファームウェアの有効化（Activate Firmware）] をクリックします。
SAS エクスパンダ ファームウェアを有効化すると、このバージョンが実行バージョンになります。

第 15 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 [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[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（Fault Summary）]タブで、次の情報を確認します。

[名前（Name）]	説明
時刻（Time）	障害が発生した時刻。

[名前（Name）]	説明
重大度（Severity）	次のいずれかになります。 • クリティカル（Critical） • 情報(Informational) • メジャー • マイナー • 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（Fault History）

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 [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[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（Fault History）]タブで、次の情報を確認します。

[名前（Name）]	説明
時刻（Time）	障害が発生した時刻。

[名前（Name）]	説明
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。

Cisco IMC ログ（Cisco IMC Log）

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 [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[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）]ウィンドウの [Cisco IMC ログ（Cisco IMC Log）] をクリックします。

ステップ 4 ログの Cisco IMCイベントごとに次の情報を確認します。

[名前（Name）]	説明
[時間（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。
[ログのクリア（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。

ステップ 5 [ページあたりのエントリ数（Entries Per Page）]ドロップダウン リストから、各ページに表示する Cisco IMC イベントの数を選択します。

ステップ 6 Cisco IMCイベントのページを前方および後方に移動するには [< 新しい（<Newer）] および [古い >（Older>）] をクリックし、リストの先頭に移動するには[<<最新（<<Newest）] をクリックします。
デフォルトでは、最新の Cisco IMCイベントがリストの先頭に表示されます。

Cisco IMCログのクリア

はじめる前に

Cisco IMCログをクリアするには、ユーザ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 [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[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 [Cisco IMC ログ（Cisco IMC Log）] をクリックします。

ステップ 4 **[Cisco IMC ログ（Cisco IMC Log）]** ペインで、[ログのクリア（Clear Log）] をクリックします。

ステップ 5 表示されるダイアログボックスで [OK]をクリックします。

システム イベント ログ（System Event Log）

システム イベント ログの表示

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[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）]ウィンドウの [システム イベント ログ（System Event Log）] をクリックします。

ステップ 4 ログ テーブルの上にパーセンテージ バーが表示され、ログ バッファがどれくらい使用されているかが示されます。

ステップ 5 ログのシステム イベントごとに次の情報を確認します。

[名前（Name）]	**説明**
[時間（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。
[ログのクリア（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。

ステップ 6 [ページあたりのエントリ数（Entries Per Page）] ドロップダウン リストから、各ページに表示するシステム イベントの数を選択します。

ステップ 7 システム イベントのページを前方および後方に移動するには [< 新しい（<Newer）]および [古い >（Older>）] をクリックし、リストの先頭に移動するには[<< 最新（<<Newest）] をクリックします。
デフォルトでは、最新のシステム イベントがリストの先頭に表示されます。

システム イベント ログのクリア

はじめる前に

システムイベントログをクリアするには、ユーザ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 [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[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）]ウィンドウの [システム イベント ログ（System Event Log）] をクリックします。

ステップ 4 [システム イベント ログ（System Event Log）]ペインで、[ログのクリア（Clear Log）] をクリックします。

ステップ 5 表示されるダイアログボックスで [OK]をクリックします。

ロギング制御

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 [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[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 コントロール（Logging Controls）] タブをクリックします。

ステップ 4 [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）] フィールドに指定された 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 5 （任意） [レポートする重大度の最小値（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）] である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 6 [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

Cisco IMCログに含まれるメッセージの最低レベルを指定できます。

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[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 コントロール（Logging Controls）] タブをクリックします。

ステップ 4 [ローカル ロギング（Local Logging）]領域で、[レポートする重大度の最小値（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）] である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 [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[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 コントロール（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 16 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

リモート サーバへのテクニカル 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）] 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 [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 サーバへのテクニカル サポート データのエクスポート（Export Technical Support Data to Remote Server）] 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 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） リモート サーバ タイプとして SCP または SFTP を選択してこのアクションを実行した場合、ポップアップ ウィンドウに「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	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。
[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 が使用する必要のあ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。

[名前（Name）]	説明
[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）] 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 [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 データの生成（Generate Technical Support Data）]オプション ボタン	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、Cisco IMC によってこのオプション ボタンがディセーブルになります。 [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。

[名前（Name）]	説明
[テクニカル サポート データの再生成（Regenerate Technical Support Data）]オプション ボタン	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、Cisco IMC によってこのオプション ボタンが表示されます。 既存のサポート データ ファイルを新しいファイルと置き換えるには、このオプションを選択し、[再生成（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 ファイルへのダウンロード（Download to local file）] オプション ボタン	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、Cisco IMC によってこのオプション ボタンがイネーブルになります。 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。
[生成（Generate）]ボタン	テクニカル サポート データ ファイルを生成できます。
[ダウンロード（Download）]ボタン	生成されたテクニカル サポート データ ファイルをダウンロードできます。

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。

Cisco IMCの再起動

現在実行されているファームウェアで問題が発生した場合など、非常に稀なケースですが、サーバのトラブルシューティング時に、Cisco IMCの再起動が必要になることがあります。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。Cisco IMCを再起動した後にログオフすると、Cisco IMC は数分間使用できません。

（注） サーバが電源投入時自己診断テスト（POST）を実行しているとき、またはExtensible Firmware Interface（EFI）シェルを操作しているときに Cisco IMCを再起動すると、サーバの電源は、Cisco IMC の再起動が完了するまでオフになります。

はじめる前に

Cisco IMCを再起動するには、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 [ユーティリティ（Utilities）]ペインの [アクション（Actions）] 領域で、[Cisco IMC の再起動（Reboot Cisco IMC）] をクリックします。

ステップ 4 [OK] をクリックします。

破損した BIOS のリカバリ

（注） この手順は、一部のサーバ モデルでは使用できません。

破損した BIOS のリカバリには、この手順の他に 3 種類の方法が存在します。

- Cisco Host Upgrade Utility（HUU）を使用する。これは推奨される方法です。
- Cisco IMCCLI インターフェイスを使用する。
- サーバのマザーボード上でハードウェア ジャンパの BIOS リカバリ機能を使用する（お使いのサーバ モデルでサポートされている場合）。手順については、お使いのサーバ モデルに対応した『Cisco UCS Server Installation and Service Guide』を参照してください。

はじめる前に

- 破損した BIOS を回復するには、admin としてログインしている必要があります。
- BIOS リカバリ ISO イメージを準備します。BIOS リカバリ ISO イメージは、ファームウェア配布パッケージの Recoveryフォルダ内にあります。
- リカバリ手順の最後にサーバの電源が再投入されるため、サーバのダウンタイムをスケジュール設定します。

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 [BIOS]をクリックします。
[BIOS] ページが表示されます。

ステップ 3 [アクション（Actions）]領域で、[破損した BIOS の回復（Recover Corrupt BIOS）] をクリックします。
[破損した BIOS の回復（Recover Corrupt BIOS）]ウィザードが表示されます。

ステップ 4 [破損した BIOS の回復（Recover Corrupt BIOS）]ウィザードを使用して、破損した BIOS を回復します。

Cisco IMCの出荷時の初期状態へのリセット

現在実行されているファームウェアで問題が発生した場合など、非常に稀なケースですが、サーバのトラブルシューティング時に、Cisco IMCの出荷時の初期状態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。Cisco IMC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、ネットワーク設定を再び指定する必要がある場合もあります。

バージョン 1.5(1) からバージョン 1.5(2) にアップグレードすると、Cisco IMCインターフェイスのホスト名はそのまま保持されます。ただし、バージョン 1.5(2) にアップグレードした後、工場出荷時の状態にリセットすると、ホスト名は CXXX-YYYYYY という形式に変更されます（XXX はサーバのモデル番号、YYYYYY はシリアル番号）。

バージョン 1.5(2) からバージョン 1.5(1) にダウングレードすると、ホスト名はそのまま保持されます。ただし、工場出荷時の状態にリセットすると、ホスト名は ucs-cxx-mx という形式に変更されます。

（注） Cisco IMC1.5(x)、2.0、および2.0(3) バージョンを工場出荷時の初期状態にリセットすると、[共有 LOM（Shared LOM）]モードがデフォルトで設定されます。C3160 サーバの場合、Cisco IMC を工場出荷時の初期状態にリセットすると、[専用（Dedicated）] モードが [フル（Full）] デュプレックスに設定され、速度はデフォルトで 100 Mbps になります。

はじめる前に

Cisco IMCを出荷時の初期状態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）] 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 [ユーティリティ（Utilities）]ペインの [アクション（Actions）] 領域で、[Cisco IMC の工場出荷時のデフォルト設定へのリセット（Reset Cisco IMC to Factory Default Configuration）] をクリックします。

ステップ 4 [OK]をクリックします。
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。

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
- 電源ポリシー
- 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

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および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）] 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 [ユーティリティ（Utilities）]ペインの [アクション（Actions）] 領域で、[Cisco IMC 設定のエクスポート（Export Cisco IMC Configuration）] をクリックします。

ステップ 4 [Cisco IMC 設定のエクスポート（Export Cisco IMC 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。

[名前（Name）]	説明
[ローカル ファイルへのエクスポート（Export to a local file）] オプション ボタン	Cisco IMC GUI を実行す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、[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 サーバへのエクスポート（Export to Remote server）]オプション ボタン	XML 設定ファイルをリモート サーバに保存するには、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。
[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） リモート サーバ タイプとして SCP または SFTP を選択してこのアクションを実行した場合、ポップアップ ウィンドウに「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 が使用する必要のあるパスおよびファイル名。

[名前（Name）]	説明
[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。次の文字は使用できません：! # $ & < > ? ; ' | ` ~ \ % ^ ( )"

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。

Cisco IMC 設定が含まれている XML ファイルでは、ネットワーク設定情報がコメントアウトされます。IP 設定情報をインポートするには、アンコメントする必要があります。ネットワーク設定をアンコメントするには、XML ファイルで次のテキストを削除します。
“□!- -Kindly Update and uncomment below settings for network configurations “ and ”- -□”

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 [ユーティリティ（Utilities）]ペインの [アクション（Actions）] 領域で、[Cisco IMC 設定のインポート（Import Cisco IMC Configuration）] をクリックします。

ステップ 4 **[Cisco IMC 設定のインポート（Import Cisco IMC 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。

[名前（Name）]	説明
[ローカル ファイルからのインポート（Import from a local file）]オプション ボタン	Cisco IMC GUI を実行するコンピュータのローカル ドライブに保存された XML 設定ファイルに移動するには、このオプションを選択し、[インポート（Import）] 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 [参照（Browse）] ボタンが表示され、インポートするファイルへの移動が可能になります。
[リモート サーバからのインポート（Import from Remote server）]オプション ボタン	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。
[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） リモート サーバ タイプとして SCP または SFTP を選択してこのアクションを実行した場合、ポップアップ ウィンドウに「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 サーバ上の設定ファイルのパスおよびファイル名。

[名前（Name）]	説明
[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）	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。次の文字は使用できません：! # $ & < > ? ; ' | ` ~ \ % ^ ( )" （注） 設定ファイルの暗号化されたセクションを編集し、これをインポートしようとすると、編集内容は無視され、インポート操作が部分的に成功したことを示す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、サーバが停止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）] 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 [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。

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。

ステップ 4 [OK] をクリックします。

Cisco IMC バナーの追加または更新

この機能を使用して、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変更できます。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 [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 [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。
[Cisco IMC バナーの追加/更新（Add/Update Cisco IMC Banner）]ポップアップ ウィンドウが表示されます。

ステップ 4 [バナー（Banner）]領域で、次の情報を確認します。

[名前（Name）]	説明
[バナー（1 行あたり 80 文字。最大 2000 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 を再起動する（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。

次の作業

Cisco IMC の最後のリセット理由の表示

この機能を使用して、コンポーネントがユーザによって最後にリセットされた理由を表示できます。

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[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 [Cisco IMC の最後のリセット（Cisco IMC Last Reset）] 領域で、次の情報を確認します。

[名前（Name）]	説明
[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。 • [ウォッチドッグリセット（watchdog-reset）]：CiscoIMC 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されます。 • [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。

セキュアなアダプタ更新の有効化

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 [セキュアなアダプタ更新（Secure Adapter Update）]領域で、[セキュアなアダプタ更新（Secure Adapter Update）] チェックボックスをオンにしてセキュアなアダプタ更新を有効にします。

（注） 更新を無効にする場合は、[セキュアなアダプタ更新（Secure Adapter Update）]チェックボックスをオフにします。

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、[ローカル ダウンロードへのハードウェア インベントリ データのダウンロード（Download Hardware Inventory Data to Local Download）] をクリックします。

ステップ 4 [ローカル ファイルへのインベントリ データのダウンロード（Download Inventory 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	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	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、Cisco IMC によってこのオプション ボタンが表示されます。
[ローカル ファイルへのダウンロード（Download to local file）]オプション ボタン	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、Cisco IMC によってこのオプション ボタンがイネーブルになります。 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、[ダウンロード] をクリックしてファイルをローカルにダウンロードします。

リモート サーバへのインベントリ ハードウェア 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 サーバへのインベントリ ハードウェア データのエクスポート（Export Inventory Hardware Data to Remote Server）] 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） リモート サーバ タイプとして SCP または SFTP を選択してこのアクションを実行した場合、ポップアップ ウィンドウに「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 が使用する必要のあ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。

第 17 章

トラブルシューティング（Troubleshooting）

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 [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 [ブートストラップ プロセスの記録（Bootstrap Process Recording）] 領域で、[記録を有効にする（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 で停止する（Stop On BIOS POST）]チェックボックスをオンにします。

ステップ 5 [変更の保存（Save Changes）]をクリックします。

ステップ 6 [ワーク（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 プロセスの記録（Bootstrap Process Recording）]ペインの [アクション（Actions）] 領域で、[記録の再生（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 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 で停止する（Stop On BIOS POST）]オプションをイネーブルにしている場合は、BIOS POST までの記録プロセスのみが再生されます。

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 プロセスの記録（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。
手順に従ってダウンロードします。

（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て事前に指定したパスに保存されます。

ステップ 10 ダウンロードが完了したら、記録のビデオを再生するファイルを選択して[開く（Open）]をクリックします。
[DVR Player 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 キャプチャの記録

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 [クラッシュ記録（Crash Recording）] 領域で、[記録を有効にする（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）] をクリックすると、クラッシュしたシステムの記録が自動的にキャプチャされます。

（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 [記録の再生（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 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。
手順に従ってダウンロードします。

（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て事前に指定したパスに保存されます。

ステップ 9 ダウンロードが完了したら、記録のビデオを再生するファイルを選択して [開く（Open）]をクリックします。
[DVR Player 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 手順に従ってダウンロードします。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、名前は次の形式です。

```
offline.tgz
```

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 でのみ必要です。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 プレーヤーが開始され、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） KVM コンソールは、[ワーク（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起動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 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 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 録画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 プレーヤーが開始され、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

この付録の構成は、次のとおりです。

C22 および C24 サーバ

C22 および C24 サーバの主要な BIOS パラメータ

[名前（Name）]	説明
[TPM サポート（TPM Support）]ドロップダウンリスト	TPM（トラステッドプラットフォーム モジュール）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ることを推奨します。

C22 および C24 サーバの高度な BIOS パラメータ

[プロセッサの設定（Processor Configuration）]のパラメータ

[名前（Name）]	説明
[Intel Hyper-Threading Technology] 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。このテクノロジーでは、マルチスレッドソフトウェアアプリケーションのスレッドを各プロセッサ内で並列に実行できます。次のいずれかになります。 • [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。 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。
[有効化されたコア数（Number of Enabled Cores）]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]～ [*n*]：サーバで実行できる物理プロセッサ 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。 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。

[名前（Name）]	説明
[Execute Disable] 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。 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。
[Intel VT] 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 VT-d] ドロップダウンリスト	Intel Virtualization Technology for Directed I/O（VT-d）をプロセッサで使用するかどうか。次のいずれかになります。 • [無効（Disabled）] : プロセッサで仮想化テクノロジーを使用しません。 • [有効（Enabled）] : プロセッサで仮想化テクノロジーを使用します。

[名前（Name）]	説明
[Intel VT-d Coherency サポート（Intel VT-d 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 VT-d ATS サポート（Intel VT-d 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。
[CPU パフォーマンス（CPU Performance）] ドロップダウンリスト	サーバの CPU パフォーマンス プロファイルを設定します。パフォーマンスプロファイルは次のオプションで構成されます。 • DCU Streamer Prefetcher • DCU IP Prefetcher • Hardware Prefetcher • Adjacent Cache-Line Prefetch 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。 • [高スループット（High Throughput）]：DCU IP Prefetcher 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。 • [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。 • [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、Hardware Prefetcher オプションと Adjacent Cache-Line Prefetch オプションは、下記のフィールドで設定できます。

[名前（Name）]	説明
[ハードウェア プリフェッチ（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 ストリーマー 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）]：DCUPrefetcher 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）]：DCUIP 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
[ダイレクト キャッシュ アクセス サポート（Direct Cache Access Support）] ドロップダウンリスト	プロセッサで、データを I/O デバイスから直接プロセッサ キャッシュに入れることにより、I/O パフォーマンスを向上させることができます。この設定はキャッシュ ミスを減らすのに役立ちます。次のいずれかになります。 • [無効（Disabled）]：データはI/O デバイスから直接プロセッサ キャッシュには入れられません。 • [有効（Enabled）]：データはI/O デバイスから直接プロセッサ キャッシュに入れられます。
[Power Technology] ドロップダウンリスト	次のオプションの CPU 電源管理設定を指定できます。 • Enhanced Intel Speedstep Technology • Intel Turbo Boost Technology • Processor Power State C6 [Power Technology] は次のいずれかになります。 • [カスタム（Custom）]：前述のBIOS パラメータの個々の設定が使用されます。これらの BIOS パラメータのいずれかを変更する場合は、このオプションを選択する必要があります。 • [無効（Disabled）]：サーバでCPU 電源管理は実行されず、前述の BIOS パラメータの設定が無視されます。 • [エネルギー効率（Energy Efficient）]：前述の BIOS パラメータに最適な設定が決定され、これらのパラメータの個々の設定は無視されます。

[名前（Name）]	説明
[Enhanced Intel Speedstep Technology] 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。このテクノロジーでは、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できます。このテクノロジーにより、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） [Power Technology] 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。
[Intel Turbo Boost Technology] 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。このテクノロジーでは、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、自動的にその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） [Power Technology] 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
[プロセッサの電源状態 C6（Processor Power State C6）]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） [Power Technology] 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。
[プロセッサの電源状態 C6 拡張（Processor Power State C1 Enhanced）]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。
[周波数フロアオーバーライド（Frequency Floor Override）]ドロップダウンリスト	アイドル時に、CPU がターボを除く最大周波数よりも低い周波数にできるようにするかどうか。次のいずれかになります。 • [無効（Disabled）]：アイドル中に CPUをターボを除く最大周波数よりも低くできます。このオプションでは電力消費が低下しますが、システムパフォーマンスが低下する可能性があります。 • [有効（Enabled）]：アイドル中にCPUをターボを除く最大周波数よりも低くできません。このオプションではシステムパフォーマンスが向上しますが、消費電力が増加することがあります。

[名前（Name）]	説明
[P-STATE Coordination] ドロップダウンリスト	BIOS がオペレーティング システムに P-state サポート モデルを通信する方法を定義できます。Advanced Configuration and Power Interface（ACPI）仕様で定義される 3 つのモデルがあります。 • [HW_ALL]：プロセッサハードウェアが、依存性のある論理プロセッサ（パッケージ内のすべての論理プロセッサ）間の P-state を調整します。 • [SW_ALL]：OS PowerManager（OSPM）が、依存性のある論理プロセッサ（物理パッケージ内のすべての論理プロセッサ）間の P-state を調整します。すべての論理プロセッサで遷移を開始する必要があります。 • [SW_ANY]：OS PowerManager（OSPM）が、依存性のある論理プロセッサ（パッケージ内のすべての論理プロセッサ）間の P-state を調整します。ドメイン内の任意の論理プロセッサで遷移を開始する場合があります。 （注） [Power Technology] 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。
[エネルギー パフォーマンス（Energy Performance）] 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。 • [バランスのとれたエネルギー（Balanced Energy）] • [バランスのとれたパフォーマンス（Balanced Performance）] • [エネルギー効率（Energy Efficient）] • [パフォーマンス（Performance）]

[メモリの設定（Memory Configuration）]のパラメータ

[名前（Name）]	説明
[メモリ RAS の選択（Select Memory RAS）]ドロップダウンリスト	サーバに対するメモリの Reliability, Availability, and Serviceability（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。 • [ミラーリング（Mirroring）]：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。 • [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。このオプションを使用した場合、[ミラーリング（Mirroring）] よりもシステム パフォーマンスが向上し、[最大パフォーマンス（Maximum Performance）] よりも信頼性が向上しますが、[ミラーリング（Mirroring）] よりも信頼性が低く、[最大パフォーマンス（Maximum Performance）] よりもシステム パフォーマンスは低下します。
[DRAM クロック スロットリング（DRAM Clock Throttling）]ドロップダウンリスト	メモリ帯域幅と消費電力に関してシステム設定を調整できます。次のいずれかになります。 • [バランス（Balanced）]：DRAMクロック スロットリングを低下させ、パフォーマンスと電力のバランスをとります。 • [パフォーマンス（Performance）]：DRAMクロックスロットリングは無効です。追加の電力をかけてメモリ帯域幅を増やします。 • [エネルギー効率（Energy Efficient）]：DRAM のクロック スロットリングを上げてエネルギー効率を向上させます。

[名前（Name）]	説明
[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）]：BIOSでNUMA をサポートしません。 • [有効（Enabled）]：NUMAに対応したオペレーティング システムに必要な ACPI テーブルを BIOS に含めます。このオプションを有効にした場合は、一部のプラットフォームでシステムのソケット間メモリインターリーブを無効にする必要があります。
[低電圧 DDR モード（Low Voltage DDR Mode）] ドロップダウンリスト	低電圧と高周波数のどちらのメモリ動作をシステムで優先するか。次のいずれかになります。 • [省電力モード（Power Saving Mode）]：低電圧のメモリ動作が高周波数のメモリ動作よりも優先されます。このモードでは、電圧を低く維持するために、メモリの周波数が低下する可能性があります。 • [パフォーマンス モード（Performance Mode）]：高周波数の動作が低電圧の動作よりも優先されます。
[DRAM リフレッシュ レート（DRAM Refresh Rate）] ドロップダウンリスト	DRAM セルをリフレッシュするレートを設定できます。次のいずれかになります。 • [1x]：DRAMセルは、64ms ごとにリフレッシュされます。 • [2x]：DRAMセルは、32ms ごとにリフレッシュされます。 • [3x]：DRAMセルは、21ms ごとにリフレッシュされます。 • [4x]：DRAMセルは、16ms ごとにリフレッシュされます。 • [自動（Auto）]：DRAMセルのリフレッシュ レートは、システム設定に基づき BIOS によって自動的に選択されます。これは、このパラメータに推奨される設定です。

[名前（Name）]	説明
[チャネル インターリーブ（Channel Interleaving）]ドロップダウンリスト	CPUがメモリ ブロックを分割して、データの隣接部分をインターリーブされたチャネル間に分散し、同時読み取り動作を有効にするかどうか。次のいずれかになります。 • [自動（Auto）]：実行するインターリーブを、CPUが決定します。 • [1 Way]：何らかのチャネル インターリーブが使用されます。 • [2 Way] • [3 Way] • [4 Way]：最大のチャネル インターリーブが使用されます。
[ランク インターリーブ（Rank Interleaving）]ドロップダウンリスト	1 つのランクを更新中に別のランクにアクセスできるよう、CPUがメモリの物理ランクをインターリーブするかどうか。次のいずれかになります。 • [自動（Auto）]：実行するインターリーブを、CPUが決定します。 • [1 Way]：一部のランクのインターリーブが使用されます。 • [2 Way] • [4 Way] • [8 Way]：ランクのインターリーブの最大容量が使用されます。

[名前（Name）]	説明
[パトロール スクラブ（Patrol Scrub）] ドロップダウンリスト	システムがサーバ上のメモリの未使用部分でも単一ビット メモリ エラーをアクティブに探して訂正するかどうか。次のいずれかになります。 • [無効（Disabled）]：CPUがメモリ アドレスの読み取りまたは書き込みを行うときのみ、システムはメモリの ECC エラーをチェックします。 • [有効（Enabled）]：システムは定期的にメモリを読み書きしてECCエラーを探します。エラーが見つかると、システムは修正を試みます。このオプションにより、単一ビット エラーは複数ビット エラーになる前に修正される場合がありますが、パトロール スクラブの実行時にパフォーマンスが低下する場合もあります。
[デマンド スクラブ（Demand Scrub）] ドロップダウンリスト	CPU または I/O が読み取りを要求した場合に検出された 1 ビットのメモリ エラーを、システムが修正するかどうか。次のいずれかになります。 • [無効（Disabled）]：1 ビットメモリ エラーは修正されません。 • [有効（Enabled）]：1 ビットメモリ エラーがメモリ内部で修正され、修正されたデータが、読み取り要求に対する応答に設定されます。
[高度（Altitude）]ドロップダウンリスト	物理サーバがインストールされているおおよその海抜（m）。次のいずれかになります。 • [自動（Auto）]：物理的な高度をCPUによって判別します。 • [300 M]：サーバは、海抜約 300 m です。 • [900 M]：サーバは、海抜約 900 m です。 • [1500 M]：サーバは、海抜約 1500 m です。 • [3000 M]：サーバは、海抜約 3000 m です。

[QPI の設定（QPI Configuration）]のパラメータ

[名前（Name）]	説明
[QPI リンク周波数選択（QPI Link Frequency Select）]ドロップダウンリスト	ギガトランスファー/秒（GT/s）単位での Intel QuickPath Interconnect（QPI）リンク周波数。次のいずれかになります。 • [自動（Auto）]：QPIリンク周波数は CPU によって決定されます。 • [6.4 GT/s] • [7.2 GT/s] • [8.0 GT/s]
[QPI スヌープ モード（QPI Snoop Mode）]ドロップダウンリスト	Intel QuickPath Interconnect（QPI）スヌープ モード。次のいずれかになります。 • [自動（Auto）]：CPUは自動的に早期スヌープ モードとして認識します。 • [早期スヌープ（Early Snoop）]：分散キャッシュリング停止で、別のキャッシング エージェントにスヌープ プローブまたは要求を直接送信できます。このモードは、遅延が少なく、スレッド全体でデータ セットを共有しているためにキャッシュ間転送からメリットが得られるワークロードや NUMA 最適化されていないワークロードに最適です。 • [ホーム スヌープ（Home Snoop）]：スヌープは、常に、メモリコントローラのホーム エージェント（集中型リング停止）によって起動されます。このモードは、早期スヌープよりローカル遅延が多いですが、未処理トランザクションが増えた場合に予備のリソースを使用できます。 • [ホーム ディレクトリ スヌープ（Home Directory Snoop）]：ホームディレクトリは、プロセッサ内の HA と iMC の両方のロジックに実装されたオプション機能です。このディレクトリの目的は、スケーラブルなプラットフォームと 2S および 4S 構成でスヌープをリモート ソケットとノード コントローラにフィルタリングすることです。 • [OSB によるホーム ディレクトリ スヌープ（Home Directory Snoop with OSB）]：OpportunisticSnoop Broadcast（OSB）ディレクトリ モードでは、HA は、ディレクトリ情報が収集されてチェックされる前であっても、非常に負荷の軽い状況下で推測的ホーム スヌープ ブロードキャストを選択できます。

[オンボード ストレージ（Onboard Storage）]のパラメータ

[名前（Name）]	説明
[オンボードSCUストレージサポート（Onboard SCU Storage Support）]ドロップダウンリスト	オンボード ソフトウェア RAID コントローラをサーバで使用できるかどうか。次のいずれかになります。 • [無効（Disabled）]：ソフトウェアRAID コントローラを使用できません。 • [有効（Enabled）]：ソフトウェアRAID コントローラを使用できます。

[USB の設定（USB Configuration）]のパラメータ

[名前（Name）]	説明
[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。 • [自動（Auto）]：USBデバイスが接続されていない場合、レガシー USB のサポートを無効にします。
[Port 60/64 エミュレーション（64 Emulation）]ドロップダウンリスト	完全な USB キーボード レガシー サポートのために 60h/64h エミュレーションをシステムでサポートするかどうか。次のいずれかになります。 • [無効（Disabled）]：60h/64エミュレーションはサポートされません。 • [有効（Enabled）]：60h/64エミュレーションはサポートされます。 サーバで USB 非対応オペレーティング システムを使用する場合は、このオプションを選択する必要があります。
[すべての USB デバイス（All USB Devices）]ドロップダウンリスト	すべての物理および仮想USBデバイスが有効であるか、無効であるか。次のいずれかになります。 • [無効（Disabled）]：すべてのUSB デバイスが無効になります。 • [有効（Enabled）]：すべてのUSB デバイスが有効です。

[名前（Name）]	説明
[USB ポート：背面（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。
[USB ポート：前面（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。
[USB ポート：内部（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。
[USB ポート：KVM（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。

[名前（Name）]	説明
[USB Port：vMedia（USB Port: vMedia）]ドロップダウンリスト	仮想メディア 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）]：vMediaデバイスを無効にします。 • [有効（Enabled）]：vMediaデバイスを有効にします。

[PCI の設定（PCI Configuration）]のパラメータ

[名前（Name）]	説明
[4 GB を超える MMIO（MMIO Above 4GB）]ドロップダウンリスト	4GB を超える MMIO を有効または無効にするかどうか。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。
[ASPM サポート（ASPM Support）]ドロップダウンリスト	BIOS での ASPM（アクティブ電源状態管理）サポートのレベルを設定できます。次のいずれかになります。 • [無効（Disabled）]：ASPMサポートは、BIOS で無効です。 • [L0 の強制（Force L0s）]：すべてのリンクを強制的にL0 スタンバイ（L0）状態にします。 • [自動（Auto）]：電力状態をCPU によって判別します。

[名前（Name）]	説明
[VGA 優先順位（VGA Priority）]	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）]：プライオリティがオンボードVGAデバイスに与えられます。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）]：プライオリティがPCIE グラフィックス アダプタに与えられます。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。 • [無効化されたオンボード VGA（Onboard VGA Disabled）]：プライオリティが PCIE グラフィックス アダプタに与えられ、オンボード VGA デバイスは無効になります。 （注） オンボード VGA が無効の場合、vKVM は機能しません。

[シリアル設定（Serial Configuration）]のパラメータ

[名前（Name）]	説明
[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。BIOS のブートが完了し、オペレーティング システムがサーバを担当すると、コンソール リダイレクションは関連がなくなり、無効になります。次のいずれかになります。 • [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。 • [有効（Enabled）]：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。

[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+]：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。 （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。
[ビット/秒（Bits per second）] 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。 • [9600]：9,600ボー レートが使用されます。 • [19200]：19,200ボー レートが使用されます。 • [38400]：38,400ボー レートが使用されます。 • [57600]：57,600ボー レートが使用されます。 • [115200]：115,200ボー レートが使用されます。 （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。
[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。 • [ハードウェア RTS/CTS（Hardware RTS/CTS）]：フロー制御に RTS/CTS が使用されます。 （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
[Putty キーパッド（Putty KeyPad）]ドロップダウンリスト	PuTTY ファンクション キーおよびテンキーの最上段のキーのアクションを変更できます。次のいずれかになります。 • [VT100]：ファンクションキーが ESC OP ～ ESC O[を生成します。 • [LINUX]：Linux仮想コンソールを模倣します。ファンクション キー F6 ～ F12 はデフォルト モードと同様に動作しますが、F1 ～ F5 は ESC [[A ～ ESC [[E を生成します。 • [XTERMR6]：ファンクションキー F5 ～ F12 がデフォルトモードと同様に動作します。ファンクション キー F1 ～ F4 が ESC OP ～ ESC OS を生成します。これはデジタル端末のキーパッドの上段によって生成されるシーケンスです。 • [SCO]：ファンクションキー F1 ～ F12 が ESC [M ～ ESC [X を生成します。ファンクションおよび Shift キーが ESC [Y ～ ESC [j を生成します。Ctrl およびファンクション キーが ESC [k ～ ESC [v を生成します。Shift、Ctrl およびファンクション キーが ESC [w ～ ESC [{ を生成します。 • [ESCN]：デフォルトモードです。ファンクション キーはデジタル端末の一般的な動作と一致します。ファンクション キーが ESC [11~ や ESC [12~ などのシーケンスを生成します。 • [VT400]：ファンクション キーがデフォルト モードと同様に動作します。テンキーの最上段のキーが ESC OP ～ ESC OS を生成します。
[BIOS POST 後にリダイレクション（Redirection After BIOS POST）]ドロップダウンリスト	BIOS POST が完了し、OS ブートローダに制御が渡された後に、BIOS コンソール リダイレクションがアクティブであるかどうか。次のいずれかになります。 • [常に有効（Always Enable）]：OS のブートおよび実行時に BIOS レガシー コンソール リダイレクションがアクティブになります。 • [ブートローダー（Bootloader）]：OSブートローダに制御が渡される前に BIOS レガシー コンソール リダイレクションが無効になります。

[名前（Name）]	説明
[アウトオブバンド管理ポート（Out-of-Band Mgmt Port）]ドロップダウンリスト	Windows 緊急管理サービスに使用可能な COM ポート 0 を設定することができます。このセットアップ オプションに基づいて ACPI SPCR テーブルが報告されます。次のいずれかになります。 • [無効（Disabled）]：Windowsオペレーティング システムで使われる汎用ポートとして COM ポート 0 を設定します。 • [有効（Enabled）]：Windows緊急管理サービス用のリモート管理ポートとして COM ポート 0 を設定します。

[LOM と PCIe スロットの設定（LOM and PCIe Slots Configuration）]のパラメータ

[名前（Name）]	説明
[すべてのオンボードLOMポート（All Onboard LOM Ports）]ドロップダウンリスト	すべての LOM ポートが有効であるか、無効であるか。次のいずれかになります。 • [無効（Disabled）]：すべてのLOM ポートが無効になります。 • [有効（Enabled）]：すべてのLOM ポートが有効です。
[LOM ポート n OptionROM（LOM Port *n* OptionROM）] ドロップダウンリスト	*n* で指定された LOM ポートでオプション 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）]：オプションROM を LOM ポート *n* では使用できません。 • [有効（Enabled）]：LOMポート *n* でオプション ROM を使用できます。 • [UEFI のみ（UEFI Only）]：拡張スロット *n* を UEFI 用でのみ使用できます。 • [レガシーのみ（Legacy Only）]：拡張スロット *n* をレガシー用でのみ使用できます。

[名前（Name）]	説明
[すべての PCIe スロットの OptionROM（All PCIe Slots OptionROM）]ドロップダウンリスト	PCIeカードのオプションROMをサーバが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PCIe スロットのオプション ROM が使用できません。 • [有効（Enabled）]：すべてのPCIe スロットのオプション ROM が使用可能です。 • [UEFI のみ（UEFI Only）]：スロット *n* のオプション ROM は UEFI にのみ使用できます。 • [レガシーのみ（Legacy Only）]：スロット *n* のオプション ROM はレガシーにのみ使用できます。
[PCIe スロット：n OptionROM（PCIe Slot:*n* OptionROM）] ドロップダウンリスト	PCIeカードのオプションROMをサーバが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。 • [UEFI のみ（UEFIOnly）][UEFI_Only]：スロット *n* のオプション ROM は UEFI にのみ使用できます。 • [レガシーのみ（LegacyOnly）][Legacy_Only]：スロット*n* のオプション ROM はレガシーにのみ使用できます。

[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	このオプションを使用すると、PCIe スロット *n* 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。 • [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。 • [無効（Disabled）]：最大速度は制限されません。 たとえば、PCIe スロット 2 にある第 3世代アダプタ カードの最大速度を、サポートされている 8GT/s の代わりに 5GT/s で実行する場合は、[PCIe スロット 2 リンク速度（PCIe Slot 2 Link Speed）] を [GEN2]に設定します。この設定により、カードでサポートされている 8GT/s の最大速度が無視され、強制的に 5GT/s の最大速度で実行されます。
[LOM に対する CDN サポート（CDN Support for LOM）]	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）]：OS イーサネット ネットワーキング識別子には、デフォルトの規則に従って ETH0、ETH1 などの名前が付けられます。デフォルトで、CDN オプションは無効です。 • [LOMS のみ（LOMS Only）]：OS イーサネット ネットワーク識別子は、LOM ポート 0 や LOM ポート 1 のように物理的な LAN on Motherboard（LOM）のポート番号付けに基づく Consistent Device Naming（CDN）による名前が付けられます。 （注） CDN は LOM ポートに対して有効であり、Windows 2012 または最新の OS のみで機能します。

[名前（Name）]	説明
[VIC に対する CDN サポート（CDN Support for VIC）]	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。 （注） VIC カードの CDN サポートは、Windows 2012 または最新の OS でのみ機能します。

C22 および C24 サーバのサーバ管理 BIOS パラメータ

[名前（Name）]	説明
[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。
[OS ウォッチドッグ タイマー（OS WatchdogTimer）] 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）] フィールドに指定された時間内にブートしない場合、Cisco IMC はエラーをログに記録し、[OS ブート ウォッチドッグ ポリシー（OS Boot Watchdog Policy）] フィールドに指定されたアクションを実行します。

[名前（Name）]	説明
[OS 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。
[OS ウォッチドッグ タイマー ポリシー（OS 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。 • [何もしない（Do Nothing）]：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、アクションは実行されません。 • [電源オフ（Power Down）]：OS のブート中にウォッチドッグ タイマーの期限が切れた場合、サーバの電源がオフになります。 • [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。

C220 および C240 サーバ

C220 および C240 サーバの主要な BIOS パラメータ

[名前（Name）]	説明
[TPM サポート（TPM Support）]ドロップダウンリスト	TPM（トラステッドプラットフォームモジュール）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ることを推奨します。

C220 および C240 サーバの高度な BIOS パラメータ

[プロセッサの設定（Processor Configuration）]のパラメータ

[名前（Name）]	説明
[Intel Hyper-Threading Technology] 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。このテクノロジーでは、マルチスレッドソフトウェアアプリケーションのスレッドを各プロセッサ内で並列に実行できます。次のいずれかになります。 • [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。 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。

[名前（Name）]	説明
[有効化されたコア数（Number of Enabled Cores）] 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]～ [*n*]：サーバで実行できる物理プロセッサ 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。 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。
[Execute Disable] 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。 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。

[名前（Name）]	説明
[Intel VT] 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 VT-d] ドロップダウンリスト	Intel Virtualization Technology for Directed I/O（VT-d）をプロセッサで使用するかどうか。次のいずれかになります。 • [無効（Disabled）]：プロセッサで仮想化テクノロジーを使用しません。 • [有効（Enabled）]：プロセッサで仮想化テクノロジーを使用します。
[Intel VT-d Coherency サポート（Intel VT-d 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 VT-d ATS サポート（Intel VT-d 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。

[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	サーバの CPU パフォーマンス プロファイルを設定します。パフォーマンス プロファイルは次のオプションで構成されます。 • DCU Streamer Prefetcher • DCU IP Prefetcher • Hardware Prefetcher • Adjacent Cache-Line Prefetch 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。 • [高スループット（High Throughput）]：DCU IP Prefetcher 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。 • [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。 • [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、Hardware Prefetcher オプションと Adjacent Cache-Line Prefetch オプションは、下記のフィールドで設定できます。
[ハードウェア プリフェッチ（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。

[名前（Name）]	説明
[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 ストリーマー 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）]：DCUPrefetcher 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）]：DCUIP 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。
[ダイレクト キャッシュ アクセス サポート（Direct Cache Access Support）] ドロップダウンリスト	プロセッサで、データを I/O デバイスから直接プロセッサ キャッシュに入れることにより、I/O パフォーマンスを向上させることができます。この設定はキャッシュ ミスを減らすのに役立ちます。次のいずれかになります。 • [無効（Disabled）]：データはI/O デバイスから直接プロセッサ キャッシュには入れられません。 • [有効（Enabled）]：データはI/O デバイスから直接プロセッサ キャッシュに入れられます。

[名前（Name）]	説明
[Power Technology] ドロップダウンリスト	次のオプションの CPU 電源管理設定を指定できます。 • Enhanced Intel Speedstep Technology • Intel Turbo Boost Technology • Processor Power State C6 [Power Technology] は次のいずれかになります。 • [カスタム（Custom）]：前述のBIOS パラメータの個々の設定が使用されます。これらの BIOS パラメータのいずれかを変更する場合は、このオプションを選択する必要があります。 • [無効（Disabled）]：サーバでCPU 電源管理は実行されず、前述の BIOS パラメータの設定が無視されます。 • [エネルギー効率（Energy Efficient）]：前述の BIOS パラメータに最適な設定が決定され、これらのパラメータの個々の設定は無視されます。
[Enhanced Intel Speedstep Technology] 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。このテクノロジーでは、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できます。このテクノロジーにより、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） [Power Technology] 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 Turbo Boost Technology] 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。このテクノロジーでは、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、自動的にその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） [Power Technology] 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。
[プロセッサの電源状態 C6（Processor Power State C6）] 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） [Power Technology] 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。
[プロセッサの電源状態 C6 拡張（Processor Power State C1 Enhanced）] 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。

[名前（Name）]	説明
[周波数フロアオーバーライド（Frequency Floor Override）] ドロップダウンリスト	アイドル時に、CPU がターボを除く最大周波数よりも低い周波数にできるようにするかどうか。次のいずれかになります。 • [無効（Disabled）]：アイドル中に CPUをターボを除く最大周波数よりも低くできます。このオプションでは電力消費が低下しますが、システムパフォーマンスが低下する可能性があります。 • [有効（Enabled）]：アイドル中にCPUをターボを除く最大周波数よりも低くできません。このオプションではシステムパフォーマンスが向上しますが、消費電力が増加することがあります。
[P-STATE Coordination] ドロップダウンリスト	BIOS がオペレーティング システムに P-state サポート モデルを通信する方法を定義できます。Advanced Configuration and Power Interface（ACPI）仕様で定義される 3 つのモデルがあります。 • [HW_ALL]：プロセッサハードウェアが、依存性のある論理プロセッサ（パッケージ内のすべての論理プロセッサ）間の P-state を調整します。 • [SW_ALL]：OS PowerManager（OSPM）が、依存性のある論理プロセッサ（物理パッケージ内のすべての論理プロセッサ）間の P-state を調整します。すべての論理プロセッサで遷移を開始する必要があります。 • [SW_ANY]：OS PowerManager（OSPM）が、依存性のある論理プロセッサ（パッケージ内のすべての論理プロセッサ）間の P-state を調整します。ドメイン内の任意の論理プロセッサで遷移を開始する場合があります。 （注） [Power Technology] 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
[エネルギー パフォーマンス（Energy Performance）]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。 • [バランスのとれたエネルギー（Balanced Energy）] • [バランスのとれたパフォーマンス（Balanced Performance）] • [エネルギー効率（Energy Efficient）] • [パフォーマンス（Performance）]

[メモリの設定（Memory Configuration）]のパラメータ

[名前（Name）]	説明
[メモリ RAS の選択（Select Memory RAS）]ドロップダウンリスト	サーバに対するメモリの Reliability, Availability, and Serviceability（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。 • [ミラーリング（Mirroring）]：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。 • [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。このオプションを使用した場合、[ミラーリング（Mirroring）] よりもシステム パフォーマンスが向上し、[最大パフォーマンス（Maximum Performance）] よりも信頼性が向上しますが、[ミラーリング（Mirroring）] よりも信頼性が低く、[最大パフォーマンス（Maximum Performance）] よりもシステム パフォーマンスは低下します。

[名前（Name）]	説明
[DRAM クロック スロットリング（DRAM Clock Throttling）]ドロップダウンリスト	メモリ帯域幅と消費電力に関してシステム設定を調整できます。次のいずれかになります。 • [バランス（Balanced）]：DRAMクロック スロットリングを低下させ、パフォーマンスと電力のバランスをとります。 • [パフォーマンス（Performance）]：DRAMクロックスロットリングは無効です。追加の電力をかけてメモリ帯域幅を増やします。 • [エネルギー効率（Energy Efficient）]：DRAM のクロック スロットリングを上げてエネルギー効率を向上させます。
[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）]：BIOSでNUMA をサポートしません。 • [有効（Enabled）]：NUMAに対応したオペレーティング システムに必要な ACPI テーブルを BIOS に含めます。このオプションを有効にした場合は、一部のプラットフォームでシステムのソケット間メモリインターリーブを無効にする必要があります。
[低電圧 DDR モード（Low Voltage DDR Mode）]ドロップダウンリスト	低電圧と高周波数のどちらのメモリ動作をシステムで優先するか。次のいずれかになります。 • [省電力モード（Power Saving Mode）]：低電圧のメモリ動作が高周波数のメモリ動作よりも優先されます。このモードでは、電圧を低く維持するために、メモリの周波数が低下する可能性があります。 • [パフォーマンス モード（Performance Mode）]：高周波数の動作が低電圧の動作よりも優先されます。

[名前（Name）]	説明
[DRAM リフレッシュ レート（DRAM Refresh Rate）]ドロップダウンリスト	DRAMセルをリフレッシュするレートを設定できます。次のいずれかになります。 • [1x]：DRAMセルは、64ms ごとにリフレッシュされます。 • [2x]：DRAMセルは、32ms ごとにリフレッシュされます。 • [3x]：DRAMセルは、21ms ごとにリフレッシュされます。 • [4x]：DRAMセルは、16ms ごとにリフレッシュされます。 • [自動（Auto）]：DRAMセルのリフレッシュ レートは、システム設定に基づき BIOS によって自動的に選択されます。これは、このパラメータに推奨される設定です。
[チャネル インターリーブ（Channel Interleaving）]ドロップダウンリスト	CPUがメモリ ブロックを分割して、データの隣接部分をインターリーブされたチャネル間に分散し、同時読み取り動作を有効にするかどうか。次のいずれかになります。 • [自動（Auto）]：実行するインターリーブを、CPU が決定します。 • [1 Way]：何らかのチャネル インターリーブが使用されます。 • [2 Way] • [3 Way] • [4 Way]：最大のチャネル インターリーブが使用されます。

[名前（Name）]	説明
[ランク インターリーブ（Rank Interleaving）]ドロップダウンリスト	1 つのランクを更新中に別のランクにアクセスできるよう、CPU がメモリの物理ランクをインターリーブするかどうか。次のいずれかになります。 • [自動（Auto）]：実行するインターリーブを、CPU が決定します。 • [1 Way]：一部のランクのインターリーブが使用されます。 • [2 Way] • [4 Way] • [8 Way]：ランクのインターリーブの最大容量が使用されます。
[パトロール スクラブ（Patrol Scrub）]ドロップダウンリスト	システムがサーバ上のメモリの未使用部分でも単一ビット メモリ エラーをアクティブに探して訂正するかどうか。次のいずれかになります。 • [無効（Disabled）]：CPUがメモリ アドレスの読み取りまたは書き込みを行うときのみ、システムはメモリの ECC エラーをチェックします。 • [有効（Enabled）]：システムは定期的にメモリを読み書きしてECCエラーを探します。エラーが見つかると、システムは修正を試みます。このオプションにより、単一ビット エラーは複数ビット エラーになる前に修正される場合がありますが、パトロール スクラブの実行時にパフォーマンスが低下する場合もあります。
[デマンド スクラブ（Demand Scrub）]ドロップダウンリスト	CPU または I/O が読み取りを要求した場合に検出された 1 ビットのメモリ エラーを、システムが修正するかどうか。次のいずれかになります。 • [無効（Disabled）]：1 ビットメモリ エラーは修正されません。 • [有効（Enabled）]：1 ビットメモリ エラーがメモリ内部で修正され、修正されたデータが、読み取り要求に対する応答に設定されます。

[名前（Name）]	説明
[高度（Altitude）]ドロップダウンリスト	物理サーバがインストールされているおおよその海抜（m）。次のいずれかになります。 • [自動（Auto）]：物理的な高度をCPUによって判別します。 • [300 M]：サーバは、海抜約 300 m です。 • [900 M]：サーバは、海抜約 900 m です。 • [1500 M]：サーバは、海抜約 1500 m です。 • [3000 M]：サーバは、海抜約 3000 m です。

[QPI の設定（QPI Configuration）]のパラメータ

[名前（Name）]	説明
[QPI リンク周波数選択（QPI Link Frequency Select）]ドロップダウンリスト	ギガトランスファー/秒（GT/s）単位での Intel QuickPath Interconnect（QPI）リンク周波数。次のいずれかになります。 • [自動（Auto）]：QPIリンク周波数は CPU によって決定されます。 • [6.4 GT/s] • [7.2 GT/s] • [8.0 GT/s]

[名前（Name）]	説明
[QPI スヌープ モード（QPI Snoop Mode）]ドロップダウンリスト	Intel QuickPath Interconnect（QPI）スヌープ モード。次のいずれかになります。 • [自動（Auto）]：CPUは自動的に早期スヌープ モードとして認識します。 • [早期スヌープ（Early Snoop）]：分散キャッシュリング停止で、別のキャッシング エージェントにスヌープ プローブまたは要求を直接送信できます。このモードは、遅延が少なく、スレッド全体でデータ セットを共有しているためにキャッシュ間転送からメリットが得られるワークロードや NUMA 最適化されていないワークロードに最適です。 • [ホーム スヌープ（Home Snoop）]：スヌープは、常に、メモリコントローラのホームエージェント（集中型リング停止）によって起動されます。このモードは、早期スヌープよりローカル遅延が多いですが、未処理トランザクションが増えた場合に予備のリソースを使用できます。 • [ホーム ディレクトリ スヌープ（Home Directory Snoop）]：ホームディレクトリは、プロセッサ内の HA と iMC の両方のロジックに実装されたオプション機能です。このディレクトリの目的は、スケーラブルなプラットフォームと 2S および 4S 構成でスヌープをリモート ソケットとノード コントローラにフィルタリングすることです。 • [OSB によるホーム ディレクトリ スヌープ（Home Directory Snoop with OSB）]：OpportunisticSnoop Broadcast（OSB）ディレクトリ モードでは、HA は、ディレクトリ情報が収集されてチェックされる前であっても、非常に負荷の軽い状況下で推測的ホーム スヌープ ブロードキャストを選択できます。

[オンボード ストレージ（Onboard Storage）]のパラメータ

[名前（Name）]	説明
[オンボード SCU ストレージ サポート（Onboard SCU Storage Support）]ドロップダウンリスト	オンボード ソフトウェア RAID コントローラをサーバで使用できるかどうか。次のいずれかになります。 • [無効（Disabled）]：ソフトウェアRAID コントローラを使用できません。 • [有効（Enabled）]：ソフトウェアRAID コントローラを使用できます。

[名前（Name）]	説明
[オンボード SCU ストレージ SW スタック（Onboard SCU Storage SW Stack）]ドロップダウンリスト	オンボード SCU ストレージ コントローラに関する Pre-boot ソフトウェア スタックを選択することができます。次のいずれかになります。 • Intel RSTe(1) • LSI SW RAID (0) （注） この設定パラメータは C220 サーバに関してのみ有効です。

[USB の設定（USB Configuration）]のパラメータ

[名前（Name）]	説明
[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。 • [自動（Auto）]：USBデバイスが接続されていない場合、レガシー USB のサポートを無効にします。
[Port 60/64 エミュレーション（64 Emulation）]ドロップダウンリスト	完全な USB キーボード レガシー サポートのために 60h/64h エミュレーションをシステムでサポートするかどうか。次のいずれかになります。 • [無効（Disabled）]：60h/64エミュレーションはサポートされません。 • [有効（Enabled）]：60h/64エミュレーションはサポートされます。 サーバで USB 非対応オペレーティング システムを使用する場合は、このオプションを選択する必要があります。
[すべての USB デバイス（All USB Devices）]ドロップダウンリスト	すべての物理および仮想USBデバイスが有効であるか、無効であるか。次のいずれかになります。 • [無効（Disabled）]：すべてのUSB デバイスが無効になります。 • [有効（Enabled）]：すべてのUSB デバイスが有効です。

[名前（Name）]	説明
[USB ポート：背面（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。
[USB ポート：前面（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。
[USB ポート：内部（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。
[USB ポート：KVM（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。

[名前（Name）]	説明
[USB Port：vMedia（USB Port: vMedia）]ドロップダウンリスト	仮想メディア 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）]：vMediaデバイスを無効にします。 • [有効（Enabled）]：vMediaデバイスを有効にします。
[USB ポート：SD カード（USB Port: SD Card）]ドロップダウンリスト	SD カード ドライブが有効か無効か。次のいずれかになります。 • [無効（Disabled）]：SDカード ドライブを無効にします。SD カード ドライブは、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 ドライブを有効にします。

[PCI の設定（PCI Configuration）]のパラメータ

[名前（Name）]	説明
[4 GB を超えるメモリ マップド I/O（Memory Mapped I/O Above 4GB）]ドロップダウンリスト	4GB を超える MMIO を有効または無効にするかどうか。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。

[名前（Name）]	説明
[MMCFG BASE] ドロップダウンリスト	4GB 以内の PCIe アダプタの低ベース アドレスを設定します。次のいずれかになります。 • 1 GB • 2 GB • 2.5 GB • 3 GB • [自動（Auto）]：自動的にPCIeアダプタの低ベースアドレスを設定します。 （注） これは C240 サーバでのみ有効です。
[ASPM サポート（ASPM Support）] ドロップダウンリスト	BIOS での ASPM（アクティブ電源状態管理）サポートのレベルを設定できます。次のいずれかになります。 • [無効（Disabled）]：ASPMサポートは、BIOS で無効です。 • [L0 の強制（Force L0s）]：すべてのリンクを強制的にL0 スタンバイ（L0）状態にします。 • [自動（Auto）]：電力状態をCPU によって判別します。
[VGA 優先順位（VGA Priority）]	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）]：プライオリティがオンボードVGA デバイスに与えられます。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）]：プライオリティがPCIE グラフィックス アダプタに与えられます。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。 • [無効化されたオンボード VGA（Onboard VGA Disabled）]：プライオリティが PCIE グラフィックス アダプタに与えられ、オンボード VGA デバイスは無効になります。 （注） オンボード VGA が無効の場合、vKVM は機能しません。

[シリアル設定（Serial Configuration）]のパラメータ

[名前（Name）]	説明
[アウトオブバンド管理ポート（Out-of-Band Mgmt Port）]ドロップダウンリスト	Windows 緊急管理サービスに使用可能な COM ポート 0 を設定することができます。このセットアップ オプションに基づいて ACPI SPCR テーブルが報告されます。次のいずれかになります。 • [無効（Disabled）]：Windowsオペレーティング システムで使われる汎用ポートとして COM ポート 0 を設定します。 • [有効（Enabled）]：Windows緊急管理サービス用のリモート管理ポートとして COM ポート 0 を設定します。
[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。BIOS のブートが完了し、オペレーティング システムがサーバを担当すると、コンソール リダイレクションは関連がなくなり、無効になります。次のいずれかになります。 • [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。 • [COM 0]：POST 中に COM ポート 0 でコンソール リダイレクションを有効にします。 • [COM 1]：POST 中に COM ポート 1 でコンソール リダイレクションを有効にします。
[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+]：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。 （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
[ビット/秒（Bits per second）] 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。 • [9600]：9,600ボー レートが使用されます。 • [19200]：19,200ボー レートが使用されます。 • [38400]：38,400ボー レートが使用されます。 • [57600]：57,600ボー レートが使用されます。 • [115200]：115,200ボー レートが使用されます。 （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。
[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。 • [ハードウェア RTS/CTS（Hardware RTS/CTS）]：フロー制御に RTS/CTS が使用されます。 （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
[Putty キーパッド（Putty KeyPad）]ドロップダウンリスト	PuTTY ファンクション キーおよびテンキーの最上段のキーのアクションを変更できます。次のいずれかになります。 • [VT100]：ファンクションキーが ESC OP ～ ESC O[を生成します。 • [LINUX]：Linux仮想コンソールを模倣します。ファンクション キー F6 ～ F12 はデフォルト モードと同様に動作しますが、F1 ～ F5 は ESC [[A ～ ESC [[E を生成します。 • [XTERMR6]：ファンクションキー F5 ～ F12 がデフォルトモードと同様に動作します。ファンクション キー F1 ～ F4 が ESC OP ～ ESC OS を生成します。これはデジタル端末のキーパッドの上段によって生成されるシーケンスです。 • [SCO]：ファンクションキー F1 ～ F12 が ESC [M ～ ESC [X を生成します。ファンクションおよび Shift キーが ESC [Y ～ ESC [j を生成します。Ctrl およびファンクション キーが ESC [k ～ ESC [v を生成します。Shift、Ctrl およびファンクション キーが ESC [w ～ ESC [{ を生成します。 • [ESCN]：デフォルトモードです。ファンクション キーはデジタル端末の一般的な動作と一致します。ファンクション キーが ESC [11~ や ESC [12~ などのシーケンスを生成します。 • [VT400]：ファンクション キーがデフォルト モードと同様に動作します。テンキーの最上段のキーが ESC OP ～ ESC OS を生成します。
[BIOS POST 後にリダイレクション（Redirection After BIOS POST）]ドロップダウンリスト	BIOS POST が完了し、OS ブートローダに制御が渡された後に、BIOS コンソール リダイレクションがアクティブであるかどうか。次のいずれかになります。 • [常に有効（Always Enable）]：OS のブートおよび実行時に BIOS レガシー コンソール リダイレクションがアクティブになります。 • [ブートローダー（Bootloader）]：OSブートローダに制御が渡される前に BIOS レガシー コンソール リダイレクションが無効になります。

[LOM と PCIe スロットの設定（LOM and PCIe Slots Configuration）]のパラメータ

[名前（Name）]	説明
[LOM に対する CDN サポート（CDN Support for LOM）]	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）]：OS イーサネット ネットワーキング識別子には、デフォルトの規則に従って ETH0、ETH1 などの名前が付けられます。デフォルトで、CDN オプションは無効です。 • [LOMS のみ（LOMS Only）]：OS イーサネット ネットワーク識別子は、LOM ポート 0 や LOM ポート 1 のように物理的な LAN on Motherboard（LOM）のポート番号付けに基づく Consistent Device Naming（CDN）による名前が付けられます。 （注） CDN は LOM ポートに対して有効であり、Windows 2012 または最新の OS のみで機能します。
[VIC に対する CDN サポート（CDN Support for VIC）]	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。 （注） VIC カードの CDN サポートは、Windows 2012 または最新の OS でのみ機能します。
[すべてのオンボード LOM ポート（All Onboard LOM Ports）] ドロップダウンリスト	すべての LOM ポートが有効であるか、無効であるか。次のいずれかになります。 • [無効（Disabled）]：すべてのLOM ポートが無効になります。 • [有効（Enabled）]：すべてのLOM ポートが有効です。

[名前（Name）]	説明
[LOM ポート n OptionROM（LOM Port *n* OptionROM）] ドロップダウンリスト	*n* で指定された LOM ポートでオプション 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。 • [UEFI のみ（UEFIOnly）][UEFI_Only]：スロット *n* のオプション ROM は UEFI にのみ使用できます。 • [レガシーのみ（LegacyOnly）][Legacy_Only]：スロット*n* のオプション ROM はレガシーにのみ使用できます。
[すべての PCIe スロットの OptionROM（All PCIe Slots OptionROM）]ドロップダウンリスト	PCIe カードのオプション ROM をサーバが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。 • [UEFI のみ（UEFIOnly）][UEFI_Only]：スロット *n* のオプション ROM は UEFI にのみ使用できます。 • [レガシーのみ（LegacyOnly）][Legacy_Only]：スロット*n* のオプション ROM はレガシーにのみ使用できます。
[PCIe スロット：n OptionROM（PCIe Slot:*n* OptionROM）] ドロップダウンリスト	PCIe カードのオプション ROM をサーバが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。 • [UEFI のみ（UEFIOnly）][UEFI_Only]：スロット *n* のオプション ROM は UEFI にのみ使用できます。 • [レガシーのみ（LegacyOnly）][Legacy_Only]：スロット*n* のオプション ROM はレガシーにのみ使用できます。

[名前（Name）]	説明
[PCIe メザニン スロット OptionROM（PCIe Mezzanine OptionROM）] ドロップダウンリスト	PCIe メザニン スロットの拡張 ROM をサーバで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。 • [UEFI のみ（UEFIOnly）][UEFI_Only]：スロット *n* のオプション ROM は UEFI にのみ使用できます。 • [レガシーのみ（LegacyOnly）][Legacy_Only]：スロット*n* のオプション ROM はレガシーにのみ使用できます。
[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	このオプションを使用すると、PCIe スロット *n* 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。 • [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。 • [無効（Disabled）]：最大速度は制限されません。 たとえば、PCIe スロット 2 にある第 3世代アダプタ カードの最大速度を、サポートされている 8GT/s の代わりに 5GT/s で実行する場合は、[PCIe スロット 2 リンク速度（PCIe Slot 2 Link Speed）] を [GEN2]に設定します。この設定により、カードでサポートされている 8GT/s の最大速度が無視され、強制的に 5GT/s の最大速度で実行されます。

C220 および C240 サーバのサーバ管理 BIOS パラメータ

[名前（Name）]	説明
[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。
[OS ウォッチドッグ タイマー（OS WatchdogTimer）] 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）] フィールドに指定された時間内にブートしない場合、Cisco IMC はエラーをログに記録し、[OS ブート ウォッチドッグ ポリシー（OS Boot Watchdog Policy）] フィールドに指定されたアクションを実行します。

[名前（Name）]	説明
[OS 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。
[OS ウォッチドッグ タイマー ポリシー（OS 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。 • [何もしない（Do Nothing）] : 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、アクションは実行されません。 • [電源オフ（Power Down）] : OS のブート中にウォッチドッグ タイマーの期限が切れた場合、サーバの電源がオフになります。 • [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。

付 録 B

複数のインターフェイスのBIOSトークン名の比較

この付録では、次の項について説明します。

複数のインターフェイスの BIOS トークン名の比較

次の表に、XML、CLI および Web GUI のインターフェイスで使用される BIOS トークン名を示します。このリストは、これらのインターフェイスに名前をマッピングするために使用できます。

（注） 使用可能なパラメータは、使用している Cisco UCS サーバのタイプによって異なります。

BIOS トークン グループ	BIOS トークン名	XML オブジェクト	CLI および Web GUI オブジェクト
メイン（Main）	TPM サポート（TPM Support）	biosVfTPMSupport/ vpTPMSupport	TPMAdminCtrl
プロセス設定（Process Configuration）	Intel(R) Hyper-Threading Technology	biosVfIntelHyperThreadingTech/ vpIntelHyperThreadingTech	IntelHyperThread
	有効なコア数（Number of Enable Cores）	biosVfCoreMultiProcessing/ vpCoreMultiProcessing	CoreMultiProcessing

BIOS トークン グループ	BIOS トークン名	XML オブジェクト	CLI および Web GUI オブジェクト
	Execute Disable	biosVfExecuteDisableBit/ vpExecuteDisableBit	ExecuteDisable
	Intel(R) VT	biosVfIntelVirtualizationTechnology/ vpIntelVirtualizationTechnology	IntelVT
	Intel(R) VT-d	biosVfIntelVTForDirectedIO/ vpIntelVTForDirectedIO	IntelVTD
	Intel(R) VT-d Coherency サポート（Intel(R) VT-d Coherency Support）	biosVfIntelVTForDirectedIO/ vpIntelVTDCoherencySupport	CoherencySupport
	Intel(R) VT-d ATS サポート（Intel(R) VT-d ATS Support）	biosVfIntelVTForDirectedIO/ vpIntelVTDATSSupport	ATS
	CPU パフォーマンス（CPU Performance）	biosVfCPUPerformance/ vpCPUPerformance	CpuPerformanceProfile
	Hardware Prefetcher	biosVfHardwarePrefetch/ vpHardwarePrefetch	HardwarePrefetch
	隣接キャッシュライン プリフェッチャ（Adjacent Cache Line Prefetcher）	biosVfAdjacentCacheLinePrefetch/ vpAdjacentCacheLinePrefetch	AdjacentCacheLinePrefetch
	DCU ストリーマプリフェッチ（DCU Streamer Prefetch）	biosVfDCUPrefetch/ vvpStreamerPrefetch	DcuStreamerPrefetch
	DCU IP Prefetcher	biosVfDCUPrefetch/ vpIPPrefetch	DcuIpPrefetch

BIOS トークン グループ	BIOS トークン名	XML オブジェクト	CLI および Web GUI オブジェクト
	ダイレクト キャッシュ アクセス サポート（Direct Cache Access Support）	biosVfDirectCacheAccess/ vpDirectCacheAccess	DirectCacheAccess
	電源技術（Power Technology）	biosVfCPUPowerManagement/ vpCPUPowerManagement	CPUPowerManagement
	Enhanced Intel Speedstep(R) Technology	biosVfEnhancedIntelSpeedStepTech/ vpEnhancedIntelSpeedStepTech	EnhancedIntelSpeedStep
	Intel(R) Turbo Boost Technology	biosVfIntelTurboBoostTech/ vpIntelTurboBoostTech	IntelTurboBoostTech
	プロセッサの電源状態 C6（Processor Power state C6）	biosVfProcessorCState/ vpProcessorCState	ProcessorC6Report
	プロセッサの電源状態 C1 拡張（Processor Power state C1 Enhanced）	biosVfProcessorC1E/ vpProcessorC1E	ProcessorC1E
	周波数フロア オーバーライド（Frequency Floor Override）	biosVfCPUFrequencyFloor/ vpCPUFrequencyFloor	CpuFreqFloor
	P-STATE 調整（P-STATE Coordination）	biosVfPStateCoordType/ vpPStateCoordType	PsdCoordType
	エネルギー パフォーマンス（Energy Performance）	biosVfCPUEnergyPerformance/ vpCPUEnergyPerformance	CpuEngPerfBias

BIOS トークン グループ	BIOS トークン名	XML オブジェクト	CLI および Web GUI オブジェクト
メモリの設定（Memory Configuration）	メモリ RAS の選択（Select Memory RAS）	biosVfSelectMemoryRASConfiguration/ vpSelectMemoryRASConfiguration	SelectMemoryRAS
	DRAM クロックスロットリング（DRAM Clock Throttling）	biosVfDRAMClockThrottling/ vpDRAMClockThrottling	DRAMClockThrottling
	NUMA	biosVfNUMAOptimized/ vpNUMAOptimized	NUMAOptimize
	低電圧 DDR モード（Low Voltage DDR Mode）	biosVfLvDIMMSupport/ vpNUMAOptimized	LvDDRMode
	DRAM リフレッシュ レート（DRAM Refresh rate）	biosVfDramRefreshRate/ vpDramRefreshRate	DramRefreshRate
	チャネル インターリーブ（Channel Interleaving）	biosVfMemoryInterleave/ vpChannelInterLeave	ChannelInterLeave
	ランク インターリーブ（Rank Interleaving）	biosVfMemoryInterleave/ vpRankInterLeave	RankInterLeave
	パトロール スクラブ（Patrol Scrub）	biosVfPatrolScrub/ vpPatrolScrub	PatrolScrub
	デマンドスクラブ（Demand Scrub）	biosVfDemandScrub/ vpDemandScrub	DemandScrub
	高度	biosVfAltitude/ vpAltitude	高度

BIOS トークン グループ	BIOS トークン名	XML オブジェクト	CLI および Web GUI オブジェクト
QPI の設定（QPI Configuration）	QPI リンク周波数選択（QPI Link Frequency Select）	biosVfQPIConfig/ vpQPILinkFrequency	QPILinkFrequency
	クラスタ オンダイ（Cluster On Die）	biosVfCODEnable/ vpCODEnable	CODEnable
	スヌープモード（Snoop Mode）	biosVfEarlySnoop/ vpEarlySnoop	EarlySnoop
SATA の設定（SATA Configuration）	SATA モード（SATA Mode）	未サポート	SATAMode
オンボードストレージ（Onboard Storage）	オンボードSCUストレージ サポート（Onboard SCU Storage Support）	biosVfOnboardStorage/ vpOnboardSCUStorageSupport	DisableSCU
	オンボードSCUストレージ SW スタック（Onboard SCU Storage SW Stack）	biosVfOnboardStorageSWStack vpOnboardSCUStorageSWStack	PchScuOromSelect
USB の設定（USB Configuration）	レガシー USB サポート（Legacy USB Support）	biosVfLegacyUSBSupport/ vpLegacyUSBSupport	LegacyUSBSupport
	ポート 60/64 エミュレーション（Port 60/64 Emulation）	biosVfUSBEmulation/ vpUSBEmul6064	UsbEmul6064
	すべての USB デバイス（All USB Devices）	biosVfUSBPortsConfig/ vpAllUsbDevices	AllUsbDevices

BIOS トークン グループ	BIOS トークン名	XML オブジェクト	CLI および Web GUI オブジェクト
	USB ポート：背面（USB Port:Rear）	biosVfUSBPortsConfig/ vpUsbPortRear	UsbPortRear
	USB ポート：前面（USB Port:Front）	biosVfUSBPortsConfig/ vpUsbPortFront	UsbPortFront
	USB ポート：内部（USB Port:Internal）	biosVfUSBPortsConfig/ vpUsbPortInternal	UsbPortInt
	USB ポート：KVM（USB Port:KVM）	biosVfUSBPortsConfig/ vpUsbPortKVM	UsbPortKVM
	USB ポート：VMedia（USB Port:VMedia）	biosVfUSBPortsConfig/ vpUsbPortVMedia	UsbPortVMedia
	USB ポート：SD カード（USB Port:SD Card）	biosVfUSBPortsConfig/ vpUsbPortSDCard	UsbPortSdCard
	xHCI モード（xHCI Mode）	biosVfPchUsb30Mode/ vpPchUsb30Mode	PchUsb30Mode
PCI の設定（PCI Configuration）	PCI ROM CLP	未サポート	PciRomClp
	4 GB を超える MMIO（MMIO above 4GB）	biosVfMemoryMappedIOAbove4GB/ vpMemoryMappedIOAbove4GB	MemoryMappedIOAbove4GB
	ASPM サポート（ASPM Support）	biosVfASPMSupport/ vpASPMSupport	ASPMSupport
	VGA 優先順位（VGA Priority）	biosVfVgaPriority/ vpVgaPriority	VgaPriority

BIOS トークン グループ	BIOS トークン名	XML オブジェクト	CLI および Web GUI オブジェクト
シリアル設定（Serial Configuration）	コンソール リダイレクション（Console Redirection）	biosVfConsoleRedirection/ vpConsoleRedirection	ConsoleRedir
	ターミナル タイプ（Terminal Type）	biosVfConsoleRedirection/ vpTerminalType	TerminalType
	ビット/秒	biosVfConsoleRedirection/ vpBaudRate	BaudRate
	フロー制御（Flow Control）	biosVfConsoleRedirection/ vpFlowControl	FlowCtrl
	Putty キーパッド（Putty KeyPad）	biosVfConsoleRedirection/ vpPuttyKeyPad	PuttyFunctionKeyPad
	BIOS POST 後にリダイレクション（Redirection After BIOS POST）	biosVfConsoleRedirection/ vpLegacyOSRedirection	RedirectionAfterPOST
LOM と PCIe スロットの設定（LOM and PCIe Slots Configuration）	PCH SATA モード（PCH SATA Mode）	biosVfSataModeSelect/ vpSataModeSelect	SataModeSelect
	すべてのオンボード LOM ポート（All Onboard LOM Ports）	biosVfSataModeSelect/ vpSataModeSelect	AllLomPortControl
	LOM ポート 0 OptionROM（LOM Port 0 OptionROM）	biosVfLOMPortOptionROM/ vpLOMPort0State	LomOpromControlPort0

BIOS トークン グループ	BIOS トークン名	XML オブジェクト	CLI および Web GUI オブジェクト
	LOM ポート 1 OptionROM（LOM Port 1 OptionROM）	biosVfLOMPortOptionROM/ vpLOMPort1State	LomOpromControlPort1
	すべての PCIe スロットの OptionROM（All PCIe Slots OptionROM）	biosVfPCIOptionROMs/ vpPCIOptionROMs	PcieOptionROMs
	PCIe スロット：*n* OptionROM（PCIe Slot:n OptionROM）	biosVfPCISlotOptionROMEnable/ vpSlot*n*State	PcieSlot*n*OptionROM
	PCIe メザニン OptionROM（PCIe Mezzanine OptionROM）	biosVfPCISlotOptionROMEnable/ vpSlotMezzState	PcieMezzOptionROM
	PCIe スロット：1 リンク速度（PCIe Slot:1 Link Speed） または SIOC1 リンク速度（SIOC1 Link Speed）	biosVfPCISlotOptionROMEnable/ vpSlot1LinkSpeed	PcieSlot1LinkSpeed
	PCIe スロット：2 リンク速度（PCIe Slot:2 Link Speed） または SIOC2 リンク速度（SIOC2 Link Speed）	biosVfPCISlotOptionROMEnable/ vpSlot2LinkSpeed	PcieSlot2LinkSpeed

BIOS トークン グループ	BIOS トークン名	XML オブジェクト	CLI および Web GUI オブジェクト
	PCIe スロット：MLOM OptionROM（PCIe Slot:MLOM OptionROM）	biosVfPCISlotOptionROMEnable/ vpSlotMLOMState	PcieSlotMLOMOptionROM
	PCIe スロット：HBA OptionROM（PCIe Slot:HBA OptionROM）	biosVfPCISlotOptionROMEnable/ vpSlotHBAState	PcieSlotHBAOptionROM
	PCIe スロット：N1 OptionROM（PCIe Slot:N1 OptionROM）	biosVfPCISlotOptionROMEnable/ vpSlotN1State	PcieSlotN1OptionROM
	PCIe スロット：N2 OptionROM（PCIe Slot:N2 OptionROM）	biosVfPCISlotOptionROMEnable/ vpSlotN2State	PcieSlotN2OptionROM
サーバ管理	FRB-2 タイマー（FRB-2 Timer）	biosVfFRB2Enable/ vpFRB2Enable	FRB-2
	OS ウォッチドッグタイマー（OS Watchdog Timer）	biosVfOSBootWatchdogTimer/ vpOSBootWatchdogTimer	OSBootWatchdogTimer
	OS ウォッチドッグタイマータイムアウト（OS Watchdog Timer Timeout）	biosVfOSBootWatchdogTimerPolicy/ vpOSBootWatchdogTimerPolicy	OSBootWatchdogTimerTimeout
	OS ウォッチドッグタイマーポリシー（OS Watchdog Timer Policy）	biosVfOSBootWatchdogTimerTimeOut/ vpOSBootWatchdogTimerPolicy	OSBootWatchdogTimerPolicy

BIOS トークン グループ	BIOS トークン名	XML オブジェクト	CLI および Web GUI オブジェクト
	ブート順序のルール（Boot Order Rules）	biosVfUCSMBootOrderRuleControl/ vpUCSMBootOrderRule	UCSMBootOrderRule

索 引

記号

B

C

F

G

H

I

K

L

N

O

P

S

T

U

V

W

X

あ

い

え

お

く

こ

さ

し

す

せ

つ

て

な

ね

は

ふ

ほ

ま

め

ゆ

り

ろ

わ