Cisco UCS C シリーズ サーバ Integrated Management Controller GUI コンフィギュレーション ガイド リリース 1.4

初版：2011 年 09 月 06 日

最終更新：2012 年 03 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/

Text Part Number: OL-23489-06-J

【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。

このマニュアルに記載されている仕様および製品に関する情報は、予告なしに変更されることがあります。 このマニュアルに記載されている表現、情報、および推奨事項は、すべて正確であると考えていますが、明示的であれ黙示的であれ、一切の保証の責任を負わないものとします。 このマニュアルに記載されている製品の使用は、すべてユーザ側の責任になります。

対象製品のソフトウェア ライセンスおよび限定保証は、製品に添付された『Information Packet』に記載されています。 添付されていない場合には、代理店にご連絡ください。

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

ここに記載されている他のいかなる保証にもよらず、各社のすべてのマニュアルおよびソフトウェアは、障害も含めて「現状のまま」として提供されます。 シスコおよびこれら各社は、商品性の保証、特定目的への準拠の保証、および権利を侵害しないことに関する保証、あるいは取引過程、使用、取引慣行によって発生する保証をはじめとする、明示されたまたは黙示された一切の保証の責任を負わないものとします。

いかなる場合においても、シスコおよびその供給者は、このマニュアルの使用または使用できないことによって発生する利益の損失やデータの損傷をはじめとする、間接的、派生的、偶発的、あるいは特殊な損害について、あらゆる可能性がシスコまたはその供給者に知らされていても、それらに対する責任を一切負わないものとします。

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: http://www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

このマニュアルで使用している IP アドレスは、実際のアドレスを示すものではありません。 マニュアル内の例、コマンド出力、および図は、説明のみを目的として使用されています。 説明の中に実際のアドレスが使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2009-2012 Cisco Systems, Inc. All rights reserved.

目 次

はじめに xi

対象読者 xi

このリリースの新規および変更情報 xi

マニュアルの構成 xii

表記法 xiii

Cisco UCS の関連ドキュメント xv

マニュアルに関するフィードバック xv

概要 1

Cisco UCS C シリーズ ラックマウント サーバの概要 1

サーバ ソフトウェアの概要 2

Cisco Integrated Management Controller 2

CIMC ユーザ インターフェイスの概要 4

CIMC ホーム ページ 4

[Navigation] ペイン 5

[Work] ペイン 6

ツールバー 9

Cisco Integrated Management Controller オンライン ヘルプの概要 10

CIMC へのログイン 10

CIMC からのログアウト 11

サーバ OS のインストール 13

OS のインストール方法 13

KVM コンソール 13

KVM コンソールを使用した OS のインストール 14

KVM コンソールを使用した OS のインストール 15

PXE インストール サーバ 15

PXE インストール サーバを使用した OS のインストール 16

サーバの管理 17

全体のサーバ ステータスの表示 17

ロケータ LED の切り替え 19

サーバのブート順の管理 20

サーバのブート順 20

サーバのブート順の設定 20

サーバの実際のブート順の表示 22

サーバのリセット 22

サーバのシャットダウン 23

サーバの電力の管理 23

サーバの電源投入 23

サーバの電源オフ 24

サーバ電源の再投入 24

電力ポリシーの設定 25

電力統計情報の表示 25

電力制限ポリシー 26

電力制限ポリシーの設定 26

電力復元ポリシーの設定 27

Flexible Flash コントローラの管理 28

Cisco Flexible Flash 28

Flexible Flash コントローラのプロパティの設定 29

Flexible Flash からのブート 30

Flexible Flash コントローラのリセット 31

BIOS の設定 32

主要な BIOS の設定 32

高度な BIOS の設定 33

サーバ管理 BIOS の設定 35

サーバのプロパティの表示 37

サーバのプロパティの表示 37

CIMC 情報の表示 38

CPU のプロパティの表示 39

メモリのプロパティの表示 39

電源のプロパティの表示 42
ストレージのプロパティの表示 42
PCI アダプタのプロパティの表示 43
サーバのセンサーの表示 45
障害の要約の表示 45
電源センサーの表示 46
ファン センサーの表示 48
温度センサーの表示 49
電圧センサーの表示 50
電流センサーの表示 51
LED センサーの表示 52
ストレージ センサーの表示 52
リモート プレゼンスの管理 55
Serial over LAN の設定 55
仮想メディアの設定 56
KVM コンソール 57
仮想 KVM の設定 58
仮想 KVM のイネーブル化 59
仮想 KVM のディセーブル化 59
ユーザ アカウントの管理 61
ローカル ユーザの設定 61
Active Directory 62
Active Directory サーバの設定 63
CIMC での Active Directory の設定 64
ユーザ セッションの表示 66
ネットワーク関連の設定 69
サーバ NIC の設定 69
サーバの NIC 69
サーバ NIC の設定 70
共通プロパティの設定 72
IPv4 の設定 72
VLAN への接続 73

ネットワーク セキュリティ設定 74
ネットワーク セキュリティ 74
ネットワーク セキュリティの設定 74
ネットワーク アダプタの管理 77
Cisco UCS C シリーズ ネットワーク アダプタの概要 77
ネットワーク アダプタのプロパティの表示 78
アダプタのプロパティの設定 81
vHBA の管理 83
vHBA の管理上の注意事項 83
vHBA のプロパティの表示 83
vHBA のプロパティの変更 88
vHBA の作成 92
vHBA の削除 93
vHBA ブート テーブル 94
ブート テーブル エントリの作成 94
ブート テーブル エントリの削除 95
vHBA の永続的なバインディング 95
永続的なバインディングの表示 96
永続的なバインディングのクリア 97
vNIC の管理 97
vNIC の管理上の注意事項 97
vNIC のプロパティの表示 98
vNIC のプロパティの変更 103
vNIC の作成 109
vNIC の削除 110
VM FEX の管理 110
仮想マシン ファブリック エクステンダ 110
仮想 FEX のプロパティの表示 110
アダプタ構成のバックアップと復元 115
アダプタ構成のエクスポート 115
アダプタ構成のインポート 116
アダプタのデフォルトの復元 117

アダプタ ファームウェアの管理 117
アダプタ ファームウェア 117
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 117
TFTP サーバからのアダプタ ファームウェアのインストール 118
アダプタ ファームウェアのアクティブ化 119
コミュニケーション サービスの設定 121
HTTP の設定 121
SSH の設定 122
XML API の設定 123
CIMC の XML API 123
XML API のイネーブル化 123
IPMI の設定 124
IPMI Over LAN 124
IPMI over LAN の設定 124
SNMP の設定 126
SNMP 126
SNMP プロパティの設定 126
SNMP トラップ設定の指定 127
SNMP テスト トラップ メッセージの送信 128
SNMPv3 ユーザの管理 129
SNMPv3 ユーザの設定 129
証明書の管理 133
サーバ証明書の管理 133
証明書署名要求の生成 134
自己署名証明書の作成 135
サーバ証明書のアップロード 137
プラットフォーム イベント フィルタの設定 139
プラットフォーム イベント フィルタ 139
プラットフォーム イベント アラートのイネーブル化 140
プラットフォーム イベント アラートのディセーブル化 140
プラットフォーム イベント フィルタの設定 140
SNMP トラップ設定の指定 142
SNMP テスト トラップ メッセージの送信 143

プラットフォーム イベント トラップの解釈 143
CIMC ファームウェア管理 147
ファームウェアの概要 147
シスコからの CIMC ファームウェアの取得 148
TFTP サーバからの CIMC ファームウェアのインストール 149
ブラウザ経由の CIMC ファームウェアのインストール 150
インストールされている CIMC ファームウェアのアクティブ化 151
TFTP サーバからの BIOS ファームウェアのインストール 152
ブラウザ経由の BIOS ファームウェアのインストール 152
ログの表示 155
CIMC ログ 155
CIMC ログの表示 155
CIMC ログのクリア 156
CIMC ログしきい値の設定 157
リモート サーバへの CIMC ログの送信 158
システム イベント ログ 159
システム イベント ログの表示 159
システム イベント ログのクリア 160
サーバ ユーティリティ 161
テクニカル サポート データのエクスポート 161
TFTP へのテクニカル サポート データのエクスポート 161
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 162
CIMC の再起動 163
破損した BIOS のリカバリ 164
CIMC の出荷時デフォルトへのリセット 165
CIMC 設定のエクスポートとインポート 165
CIMC 設定のエクスポートとインポート 165
CIMC 設定のエクスポート 166
CIMC 設定のインポート 167
サーバ モデル別 BIOS パラメータ 169
C200 および C210 サーバ 169
C200 および C210 サーバの主要な BIOS パラメータ 169

C200 および C210 サーバの高度な BIOS パラメータ 170
C200 および C210 サーバのサーバ管理 BIOS パラメータ 183
C250 サーバ 186
C250 サーバの主要な BIOS パラメータ 186
C250 サーバの高度な BIOS パラメータ 187
C250 サーバのサーバ管理 BIOS パラメータ 198
C260 サーバ 201
C260 サーバの主要な BIOS パラメータ 201
C260 サーバの高度な BIOS パラメータ 202
C260 サーバのサーバ管理 BIOS パラメータ 213
C460 サーバ 217
C460 サーバの主要な BIOS パラメータ 217
C460 サーバの高度な BIOS パラメータ 218
C460 サーバのサーバ管理 BIOS パラメータ 229

はじめに

この前書きは、次の項で構成されています。

- 対象読者，xi ページ
- このリリースの新規および変更情報，xi ページ
- マニュアルの構成，xii ページ
- 表記法，xiii ページ
- Cisco UCS の関連ドキュメント，xv ページ
- マニュアルに関するフィードバック，xv ページ

対象読者

このガイドは、次の 1 つ以上に責任と専門知識を持つ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

このリリースの新規および変更情報

次の表に、最新リリースに関するこのガイドでの重要な変更点の概要を示します。 この表は、コンフィギュレーション ガイドに加えられたすべての変更、またはこのリリースの新機能をすべて網羅したリストを示すものではありません。 このリリースで新しくサポートされるハードウェアの詳細については、Cisco UCS C-Series Servers Documentation Roadmap から入手できる『*Release Notes for Cisco UCS C-Series Rack-Mount Servers*』を参照してください。

機能	説明	参照先
VM FEX	仮想マシン ファブリック エクステンダ（VM FEX）のサポートが追加されました。	ネットワーク アダプタの管理, （77 ページ）
vHBA の作成	最大 16 個の vHBA を作成するためのサポートが CLI に追加されました。	ネットワーク アダプタの管理, （77 ページ）
Active Directory グループ	Active Directory 権限付与グループのサポートが追加されました。	ユーザ アカウントの管理, （61 ページ）
拡張された SNMP 機能	SNMPv3 のサポートが拡張され、SNMP トラップ コンフィギュレーションがユーザ インターフェイスで再配置されました。	コミュニケーション サービスの設定, （121 ページ）
XML API	XML API による CIMC 制御のサポートが追加されました。	コミュニケーション サービスの設定, （121 ページ）
HTTP リダイレクト	HTTP 要求の HTTPS へのリダイレクションを設定できます。	コミュニケーション サービスの設定, （121 ページ）

マニュアルの構成

このマニュアルの構成は、次のとおりです。

章	タイトル	説明
第 1 章	概要	Cisco UCS C シリーズ ラックマウント サーバおよび CIMC CLIGUI について説明します。
第 2 章	サーバ OS のインストール	サーバでオペレーティング システム（OS）を設定する方法について説明します。
第 3 章	サーバの管理	ブート デバイスの順序の設定、サーバへの電力の制御、およびサーバのリセット方法を説明します。
第 4 章	サーバのプロパティの表示	サーバの CPU、メモリ、電源、ストレージ、および PCI アダプタのプロパティの表示方法について説明します。
第 5 章	サーバのセンサーの表示	電源、ファン、温度、電圧、電流、およびストレージのセンサーの表示方法について説明します。

章	タイトル	説明
第 6 章	リモート プレゼンスの管理	仮想 KVM、仮想メディア、および Serial over LAN 接続の設定方法を説明します。
第 7 章	ユーザ アカウントの管理	ユーザ アカウントの追加または変更方法、ユーザを認証するための Active Directory の設定方法、およびユーザ セッションの管理方法について説明します。
第 8 章	ネットワーク関連の設定	ネットワーク インターフェイス、ネットワーク設定、およびネットワーク セキュリティの設定方法を説明します。
第 9 章	ネットワーク アダプタの管理	ネットワーク アダプタを作成、設定、および管理する方法について説明します。
第 10 章	コミュニケーション サービスの設定	HTTP、SSH、IPMI、XML API、および SNMP によるサーバ管理コミュニケーションの設定方法について説明します。
第 11 章	証明書の管理	サーバ証明書を生成、アップロード、および管理する方法を説明します。
第 12 章	プラットフォーム イベント フィルタの設定	プラットフォーム イベント フィルタの設定および管理方法について説明します。
第 13 章	CIMC ファームウェア管理	ファームウェア イメージを取得、インストール、およびアクティブにする方法を説明します。
第 14 章	ログの表示	CIMC およびシステム イベント ログ メッセージを表示、エクスポート、およびクリアする方法について説明します。
第 15 章	サーバ ユーティリティ	サポート データをエクスポートする方法、BIOS をクリアまたは回復する方法、サーバの設定を出荷時の初期状態にリセットする方法、設定をバックアップする方法、および管理インターフェイスをリブートする方法について説明します。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	用途
太字フォント	コマンド、キーワード、およびユーザが入力したテキストは、**太字**フォントで示しています。
イタリック体フォント	ドキュメント名、新規用語または強調する用語、値を指定するための引数は、イタリック体フォントで示しています。
courier フォント	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。
[ ]	角カッコの中の要素は、省略可能です。
{x | y | z}	いずれか 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。

ヒント 「問題解決に役立つ情報」です。

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。

ワンポイント アドバイス	時間を節約する方法です。 ここに紹介している方法で作業を行うと、時間を短縮できます。
警告	読者に対する警告を意味します。 人身事故を予防するための注意事項が記述されています。

Cisco UCS の関連ドキュメント

ドキュメント ロードマップ

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

C シリーズのすべてのマニュアルの一覧については、次の URL から入手できる『*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

その他のドキュメント リソース

B シリーズおよび C シリーズのマニュアルをすべて含む ISO ファイルは、次の URL で入手できます。http://www.cisco.com/cisco/software/type.html?mdfid=283853163&flowid=25821。 このページから、[Unified Computing System (UCS) Documentation Roadmap Bundle] をクリックします。

ISO ファイルは、マニュアルのメジャー リリースごとに更新されます。

マニュアル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。

マニュアルに関するフィードバック

このマニュアルに関する技術的なフィードバック、または誤りや記載漏れに関する報告は、ucs-docfeedback@external.cisco.com に送信してください。 フィードバックをお待ちしています。

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，1 ページ
- サーバ ソフトウェアの概要，2 ページ
- Cisco Integrated Management Controller，2 ページ
- CIMC ユーザ インターフェイスの概要，4 ページ

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 C200 ラックマウント サーバ
- Cisco UCS C210 ラックマウント サーバ
- Cisco UCS C250 ラックマウント サーバ
- Cisco UCS C260 ラックマウント サーバ
- Cisco UCS C460 ラックマウント サーバ

（注） このファームウェア リリースでサポートされている Cisco UCS C シリーズ ラックマウント サーバを確認するには、『*Release Notes for Cisco Integrated Management Controller*』を参照してください。

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、出荷時に 2 つの主要なソフトウェア システムがインストールされています。

CIMC ファームウェア

CIMC 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。 メイン サーバ CPU とは別の専用の ARM ベース プロセッサによって CIMC ファームウェアが実行されます。 システムには CIMC ファームウェアの実行バージョンが付属しています。 CIMC 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ありません。

サーバ OS

メイン サーバ CPU によって Windows や Linux などの OS が実行されます。 サーバには出荷時に OS が事前インストールされていますが、DVD ドライブまたはネットワークを使用して別の OS をインストールできます。 CIMC を使用すると、KVM コンソールおよび vMedia を使用して新しい OS をインストールできます。

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

Cisco Integrated Management Controller

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

（注） CIMC 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のみ使用します。 C シリーズ サーバが UCS システムに統合された場合は、UCS Manager を使用して管理する必要があります。 UCS Manager の使用の詳細については、http://www.cisco.com/go/unifiedcomputing/b-series-doc の『*Cisco UCS B-Series Servers Documentation Roadmap*』に記載されているコンフィギュレーション 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 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。

- CIMC GUI を使用して CIMC CLI を呼び出す
- CIMC CLI で呼び出したコマンドを CIMC GUI に表示する

- CIMC GUI から CIMC CLI の出力を生成する

CIMC で実行可能なタスク

CIMC を使用すると次のサーバ管理タスクを実行できます。

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

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

CIMC 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 CIMC 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

CIMC ユーザ インターフェイスの概要

CIMC 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。 CIMC 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。

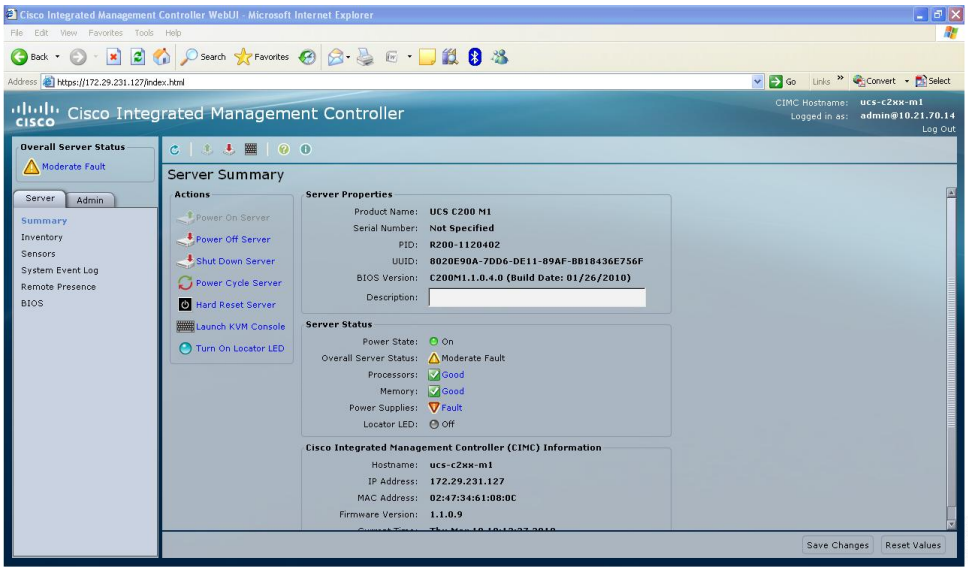
- Java 1.6 以降
- HTTP および HTTPS 対応
- Adobe Flash Player 10 以降

（注） CIMC 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 の『*Cisco UCS C-Series Servers Documentation Roadmap*』から入手できます。

CIMC ホーム ページ

図 1 は CIMC のホーム ページです。

図 *1* : *CIMC* ホーム ページ



[Navigation] ペイン

[Navigation] ペインは、CIMC ユーザ インターフェイスの左側に表示されます。 [Navigation] ペインで [Server] タブまたは [Admin] タブのリンクをクリックすると、CIMC ユーザ インターフェイスの右側の [Work] ペインに選択したページが表示されます。

次の表では、[Navigation] ペインの要素について説明します。

要素名	説明
[Overall Server Status] 領域	[Overall Server Status] 領域は、[Server] タブおよび[Admin] タブの上にあります。 この領域をクリックすると、[Server Summary] ページがリフレッシュされます。
[Server] タブ	[Server] タブは、[Navigation] ペインにあります。 このタブには次のページへのリンクが含まれます。 • **Summary** • **Inventory** • **Sensor** • **System Event Log** • **Remote Presence** • **BIOS** • **Power Policies** • **Faults Summary**
[Admin] タブ	[Admin] タブは、[Navigation] ペインにあります。 このタブには次のページへのリンクが含まれます。 • **User Management** • **Network** • **Communications Services** • **Certificate Management** • **CIMC Log** • **Event Management** • **Firmware Management** • **Utilities**

[Work] ペイン

[Work] ペインは、UI の右側に表示されます。 [Work] ペインには、[Server] タブまたは [Admin] タブでクリックしたリンクに応じて異なるページが表示されます。

次の表は、[Work] ペインの要素とページをまとめたものです。

ページまたは要素名	説明
Summary	このページには 4 つの領域があります。 • [Actions]：この領域では、サーバの電源の制御、サーバのリセット、KVM コンソールの起動、またはロケータ LED の制御を行います。 • [Server Properties]：この領域には、一般的なサーバ プロパティが表示され、サーバの説明を割り当てます。 • [Server Status]：この領域には、主要なサーバ サブシステムの全体的なステータスが表示されます。 • [CIMC Information]：この領域には、サーバ管理名、ネットワーク アドレス、ファームウェア バージョン、および現在の日付と時刻が表示されます。
Inventory	このページには 6 つのタブがあります。 • [CPUs]：このタブには、CPU についての情報が表示されます。 • [Memory]：このタブには、メモリについての情報が表示されます。 • [Power Supplies]：このタブには、電源についての情報が表示されます。 • [Network Adapters]：このタブには、ネットワーク アダプタについての情報が表示されます。 • [Storage]：このタブには、ストレージについての情報が表示されます。 • [PCI Adapters]：このタブには、PCI アダプタについての情報が表示されます。

Sensor	このページには 7 つのタブがあります。 • [Power Supply]：このタブには、電源センサーが表示されます。 • [Fan]：このタブには、ファン センサーが表示されます。 • [Temperature]：このタブには、温度センサーが表示されます。 • [Voltage]：このタブには、電圧センサーが表示されます。 • [Current]：このタブには、電流センサーが表示されます。 • [LEDs]：このタブには、LED の状態および色が表示されます。 • [Storage]：このタブには、ストレージデバイスの状態が表示されます。
System Event Log	このページには、システム イベント ログが表示されます。
Remote Presence	このページには 3 つのタブがあります。 • [Virtual KVM]：このタブでは、vKVM のプロパティを設定します。 • [Virtual Media]：このタブでは、仮想メディアのプロパティを設定します。 • [Serial over LAN]：このタブでは、Serial over LAN のプロパティを設定します。
BIOS	このページには 3 つの領域があります。 • [Actions]：この領域では、サーバのブート順の設定、壊れた BIOS のリカバリ、および BIOS CMOS のクリアを行います。 • [BIOS Properties]：この領域には BIOS の実行されているバージョンが表示されます。 • [Boot Order]：この領域には、設定されているブート順と実際のブート順が表示されます。
Power Policies	このページには 2 つの領域があります。 • [Power Usage]：この領域には、電力統計情報が表示され、サーバの電力消費の制限を設定します。 • [Power Restore Policy]：この領域では、停止後のサーバの電力の復元方法を設定します。

Fault Summary	このページには 2 つの領域があります。 • [Discrete Sensors]：この領域には、離散センサーの状態が表示されます。 • [Threshold Sensors]：この領域には、しきい値センサーの状態が表示されます。
User Management	このページには 3 つのタブがあります。 • [Local Users]：このタブでは、ユーザ アカウントを作成または変更します。 • [Active Directory]：このタブでは、Active Directory のプロパティを設定します。 • [Sessions]：このタブには、現在のユーザ セッションが表示されます。
Network	このページには 2 つのタブがあります。 • [Network Settings]：このタブでは、ネットワーク プロパティを設定します。 • [Network Security]：このタブでは、ネットワーク セキュリティを設定します。
Communications Services	このページには 2 つの領域があります。 • [Communications Services]：この領域では、HTTP、SSH、XML API、および IPMI over LAN のプロパティを設定します。 • [SNMP]：この領域では、SNMP のプロパティを設定します。
Certificate Management	このページには 2 つの領域があります。 • [Actions]：この領域では、証明書を生成してアップロードします。 • [Current Certificate]：この領域には、サーバの現在の証明書が表示されます。
CIMC Log	このページには 2 つのタブがあります。 • [CIMC Log]：このタブには、CIMC ログが表示されます。 • [Remote Logging]：このタブでは、リモート Syslog サーバへのログ メッセージの送信を設定します。

Event Management	このページには 1 つのタブがあります。 • [Platform Event Filters]：このタブでは、プラットフォーム イベント フィルタを設定します。
Firmware Management	このページには 3 つの領域があります。 • [Actions]：この領域では、クライアントブラウザまたはTFTPサーバからCIMCファームウェアをインストールするか、またはインストールされている CIMC ファームウェアをアクティブにします。 • [CIMC Firmware]：この領域には、ファームウェアの実行、バックアップ、およびブートローダのバージョンのステータスが表示されます。 • [Last Firmware Install]：この領域には、ファームウェアの最後の更新に関する情報が表示されます。
Utilities	このページには 3 つの領域があります。 • [Actions]：この領域では、テクニカル サポート データをエクスポートし、CIMC設定をエクスポートまたはインポートし、CIMC を出荷時の初期状態にリセットし、CIMC をリブートします。 • [Last Technical Support Data Export]：この領域には、テクニカル サポート データの最後のエクスポートに関する情報が表示されます。 • [CIMC Configuration Import/Export]：この領域には、アクション タイプとそのステータスが表示されます。

ツールバー

ツールバーは [Work] ペインの上に表示されます。

要素名	説明
Refresh	現在のページを更新します。
Power On Server	サーバの電源を投入します。
Power Off Server	サーバの電源を切ります。
Launch KVM Console	KVM コンソールを起動します。

Help	ヘルプを表示します。
Info	CIMC 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 は、左側の [Navigation] ペインと右側の [Work] ペインの 2 つの主要なセクションに分かれています。

このヘルプ システムは、各 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。

ヘルプ ページにアクセスするには、次の操作を実行します。

- GUI の特定のタブで、[Work] ペイン上方のツールバーにある [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 [Help] ボタンをクリックします。

（注） C シリーズのすべてのマニュアルの一覧については、次の URL から入手できる『*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

CIMC 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、CIMC 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) [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最初にログインするときは、ユーザ名として **admin** を使用し、パスワードとして **password** を使用します。

ステップ 4 [Log In] をクリックします。

CIMC からのログアウト

手順

ステップ 1 CIMC の右上で、[Log Out] をクリックします。
ログアウトすると、CIMC 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，13 ページ
- KVM コンソール，13 ページ
- PXE インストール サーバ，15 ページ

OS のインストール方法

C シリーズ サーバは、複数のオペレーティング システムをサポートしています。インストールされている OS に関係なく、次のいずれかのツールを使用してサーバにインストールできます。

- KVM コンソール
- PXE インストール サーバ

KVM コンソール

KVM コンソールは CIMC 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 上の 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。 この場合は、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] セクションで [Do not save encrypted pages to disk] の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。

（注） KVM コンソールは、GUI からのみ操作します。 KVM コンソールを起動するには、『*Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide*』の手順を参照してください。

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 CIMC が開いていない場合は、ログインします。

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

ステップ 4 [Server] タブの [Remote Presence] をクリックします。

ステップ 5 [Remote Presence] ペインの [Virtual KVM] タブをクリックします。

ステップ 6 [Actions] 領域で、[Launch KVM Console] をクリックします。

[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 [Mapped] チェックボックスをオンにします。
- [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。[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 [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。 タブを閉じると、すべての仮想メディアのマッピングが解除されます。

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

次の作業

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

KVM コンソールを使用した OS のインストール

KVM コンソールは GUI によってのみ操作されるため、CLI を使用してサーバ OS をインストールすることはできません。 KVM コンソールを使用して OS をインストールするには、『*Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide*』の「Installing an OS Using the KVM Console」の項の手順に従います。

（注） 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

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。

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，17 ページ
- ロケータ LED の切り替え，19 ページ
- サーバのブート順の管理，20 ページ
- サーバのリセット，22 ページ
- サーバのシャットダウン，23 ページ
- サーバの電力の管理，23 ページ
- 電力ポリシーの設定，25 ページ
- Flexible Flash コントローラの管理，28 ページ
- BIOS の設定，32 ページ

全体のサーバ ステータスの表示

手順

ステップ 1 [Navigation] ペインの [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、[Server Summary] ペインを更新します。

ステップ 2 （任意） [Server Summary] ペインの [Server Status] 領域で、次の情報を確認します。

（注） 次のリストに、表示される可能性が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	説明
[Power State] フィールド	現在の電源状態。

名前	説明
[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。 • [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 • Moderate Fault • Severe Fault
[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 • 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。
[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。
[Memory] 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 • 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	説明
[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 • 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。
[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 • 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。
[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。
[Locator LED] フィールド	ロケータ LED がオンかオフか。

ロケータ LED の切り替え

はじめる前に

この操作を含むすべての電力制御操作には、ユーザ権限が必要になります。

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Summary] をクリックします。

ステップ 3 [Actions] 領域で、[Turn On Locator LED] をクリックします。
ロケータ LED がオンになり、点滅します。

ステップ 4 [Actions] 領域で、[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。

サーバのブート順の管理

サーバのブート順

CIMC 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。

ブート順の設定を変更すると、CIMC 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、設定が再度変更されるまで再送信されません。

（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。

サーバのブート順の設定

はじめる前に

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

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [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 [Actions] 領域で、[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。
[Configure Boot Order] ダイアログボックスが表示されます。

ステップ 5 [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	説明
[Device Types] テーブル	サーバのブート オプション。 次の 1 つ以上を選択できます。 • [HDD]：ハード ディスク ドライブ • [FDD]：フロッピー ディスク ドライブ • [CDROM]：ブート可能な CD-ROM • [PXE]：PXE ブート • [EFI]：Extensible Firmware Interface
Add >	選択したデバイス タイプを [Boot Order] テーブルに移動します。
< Remove	選択したデバイス タイプを [Boot Order] テーブルから削除します。
[Boot Order] テーブル	このサーバがブートできるデバイス タイプが、ブートが試行される順番に表示されます。
Up	選択したデバイス タイプを [Boot Order] テーブルで高いプライオリティに移動します。
Down	選択したデバイス タイプを [Boot Order] テーブルで低いプライオリティに移動します。
[Apply] 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。 CIMC は、サーバが次に再起動されるときに、設定されているブート順を BIOS に送信します。

名前	説明
[Cancel] ボタン	変更を保存しないで、または既存の設定を再適用しないで、ダイアログボックスを閉じます。 このオプションを選択すると、サーバが次に再起動されるときに、実際のブート順は変更されません。

ステップ 6 [Apply] 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。

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、CIMC 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 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [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 [Actual Boot Order] 領域で、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順序になっている、ブート デバイスのリストを確認します。
同じデバイス タイプの複数のインスタンスが最後のブート時に存在していた場合は、デバイス タイプを展開してそれらのデバイスを確認できます。

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、ユーザ権限または admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Summary] をクリックします。

ステップ 3 [Actions] 領域で、[Hard Reset Server] をクリックします。
[Hard Reset the Server?] というメッセージ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 [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、ユーザ権限または admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Summary] をクリックします。

ステップ 3 [Actions] 領域で、[Shut Down Server] をクリックします。
[Shut Down the Server?] というメッセージ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 [OK] をクリックします。

サーバの電力の管理

サーバの電源投入

（注） サーバの電源がCIMC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、CIMC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、ユーザ権限または admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Summary] をクリックします。

ステップ 3 [Actions] 領域で、[Power On Server] をクリックします。
[Power on the server?] というメッセージ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 [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、ユーザ権限または admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Summary] をクリックします。

ステップ 3 [Actions] 領域で、[Power Off Server] をクリックします。
[Power Off the Server?] というメッセージ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 [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、ユーザ権限または admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Summary] をクリックします。

ステップ 3 [Actions] 領域で、[Power Cycle Server] をクリックします。
[Power Cycle the Server?] というメッセージ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 [OK] をクリックします。

電力ポリシーの設定

電力統計情報の表示

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Power Policies] をクリックします。

ステップ 3 [Power Statistics] 領域で、次のフィールドの情報を確認します。

名前	説明
[Current Consumption] フィールド	サーバによって現在使用されている電力（ワット単位）。
[Maximum Consumption] フィールド	サーバが最後にリブートされてから使用した最大ワット数。
[Minimum Consumption] フィールド	サーバが最後にリブートされてから使用した最小ワット数。
[Minimum Configurable Limit] フィールド	このサーバのピーク時の電力制限として指定できる最小電力（ワット単位）。
[Maximum Configurable Limit] フィールド	このサーバのピーク時の電力制限として指定できる最大電力（ワット単位）。

電力制限ポリシー

電力制限ポリシーによって、サーバの電力消費をアクティブに管理する方法が決定されます。 電力制限をイネーブルにすると、サーバに割り当てられている電力量がモニタされ、割り当てられている電力未満に電力消費を抑えることが試行されます。 サーバがその最大割り当てを超過すると、電力制限ポリシーによって、指定された違反アクションがトリガーされます。

電力制限ポリシーの設定

（注） この機能は、一部のサーバでは使用できません。

はじめる前に

このタスクを実行するには、ユーザ権限または admin 権限を使用してログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Power Policies] をクリックします。

ステップ 3 [Power Configuration] 領域で、次のプロパティを更新します。

名前	説明
[Enable Power Capping] チェックボックス	オンにすると電力制限をイネーブルにすると、サーバに割り当てられている電力量がモニタされ、サーバが最大割り当て量を超えた場合に指定したアクションが実行されます。
[Peak Power] フィールド	このサーバに割り当て可能な最大ワット数。 このフィールドに指定された値よりも多い電力量をサーバが要求すると、[Non-Compliance Action] フィールドに定義されているアクションが実行されます。 [Minimum Configurable Limit] フィールドと [Maximum Configurable Limit] フィールドで定義した範囲内のワット数を入力します。

名前	説明
[Non-Compliance Action] ドロップダウン リスト	電力制限がイネーブルで、サーバがピーク時の電力割り当て量を超える電力を要求した場合に実行されるアクション。次のいずれかになります。 • [Force Power Reduction]**force-power-reduction**：サーバは何らかの方法で電力消費を削減する必要があります。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。 • [None]**none**：アクションは実行されず、サーバは [Peak Power] フィールドに指定された値以上の電力を使用できます。 • [Power Off Host]**power-off-host**：サーバはシャットダウンされます。 • [Throttle]**throttle**：サーバで実行されているプロセスは、合計電力消費を少なくするように抑制されます。

ステップ 4 [Save Changes] をクリックします。

電力復元ポリシーの設定

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

はじめる前に

このタスクを実行するには、ユーザ権限または admin 権限を使用してログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Power Policies] をクリックします。

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

名前	説明
[Power Restore Policy] ドロップダウン リスト	予期しない電力損失後にシャーシ電源が復帰し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。 • [Power Off]**power-off**：サーバの電源は手動で再起動されるまでオフのままです。 • [Power On]**power-on**：サーバは電源が復帰したときに通常どおり起動できます。 サーバはただちに再起動するか、オプションで固定長遅延またはランダムな長さの遅延の後に再起動できます。 • [Restore Last State]**restore-last-state**：サーバは再起動し、システムは電源損失前に実行されていたプロセスを復元しようとします。
[Power Delay Type] ドロップダウン リスト	選択したポリシーが [Power On]**power-on** の場合、このオプションで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。 • [fixed]：サーバは固定長遅延の後に再起動されます。 • [random]：サーバはランダムな長さの遅延の後に再起動されます。
[Power Delay Value] フィールド	固定長遅延を選択した場合、シャーシ電源が復帰してからサーバが再起動されるまでの秒数。 0 ～ 240 の整数を入力します。

ステップ 4 [Save Changes] をクリックします。

Flexible Flash コントローラの管理

Cisco Flexible Flash

一部の C シリーズ ラックマウント サーバは、サーバ ソフトウェア ツールおよびユーティリティのストレージとして、内部 Secure Digital（SD）メモリ カードをサポートします。 SD カードは、Cisco Flexible Flash ストレージ アダプタによってホストされます。

SD ストレージは、CIMC では 4 つの仮想 USB ドライブとして使用できます。 3 つは Cisco ソフトウェアによってあらかじめロードされ、4 つ目にはユーザがインストールしたハイパーバイザまたはその他のコンテンツを保持できます。 4 つの仮想ドライブは次のとおりです。

- Cisco UCS Server Configuration Utility（ブート可能）
- ユーザ インストール（ブート可能の場合がある）
- シスコ ドライバ（ブート不可能）
- Cisco Host Upgrade Utility（ブート可能）

シスコのソフトウェア 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 にある『*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

Flexible Flash コントローラのプロパティの設定

はじめる前に

- このタスクを実行するには、ユーザ権限または admin 権限を使用してログインする必要があります。
- Cisco Flexible Flash がプラットフォームでサポートされている必要があります。

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Inventory] をクリックします。

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

ステップ 4 [Storage Adapters] テーブルで、FlexFlash コントローラをクリックします。
選択した FlexFlash コントローラのプロパティが、[Storage Adapters] 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 [Storage Card] タブ付きメニューで、[Controller Info] タブをクリックします。

ステップ 6 [Actions] 領域で、[Configure Operational Profile] をクリックします。
[Operational Profile] ダイアログボックスが開きます。

ステップ 7 [Operational Profile] ダイアログボックスで、次のフィールドを更新します。

名前	説明
[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。

名前	説明
[Virtual Drives Enabled] フィールド	USB スタイルのドライブとしてサーバで使用可能にすることができる仮想ドライブ。 サーバでアクセスする各仮想ドライブの横のボックスをオンにします。 次のオプションがあります。 • [SCU]：サーバは Cisco UCS Server Configuration Utility にアクセスできます。 • [Drivers]：サーバは Cisco ドライバにアクセスできます。 • [HV]：サーバはユーザがインストールしたハイパーバイザにアクセスできます。 • [HUU]：サーバは Cisco Host Upgrade Utility にアクセスできます。
[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。 **重要** 現在、スロット 1 では Cisco Flexible Flash カードのみがサポートされています。 そのため、このフィールドは slot1 に設定する必要があります。
[Error Count 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/書き込みエラーの数。 エラーの数がこのしきい値を超えると、Cisco FlexFlash カードはディセーブルになります。 読み取り/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。 発生したエラーの数にかかわらずカードがディセーブルにならないようにするには、0（ゼロ）を入力します。

ステップ 8 [Save Changes] をクリックします。

Flexible Flash からのブート

サーバに対して定義された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るときにデフォルトのブート プライオリティを上書きするブート可能仮想ドライブを、Cisco Flexible Flash カード上に指定できます。 指定したブート デバイスは 1 回のみ使用されます。 サーバがリブートされた後は、この設定は無視されます。

（注） サーバをリブートする前に、選択した仮想ドライブが Cisco Flexible Flash カード上でイネーブルであることを確認します。 これを確認するには、[Storage] タブに移動し、カードを選択して、[Virtual Drive Info] サブタブに移動します。

はじめる前に

- このタスクを実行するには、ユーザ権限または admin 権限を使用してログインする必要があります。
- Cisco Flexible Flash がプラットフォームでサポートされている必要があります。

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [BIOS] をクリックします。

ステップ 3 [Actions] 領域で、[Configure Boot Override Priority] をクリックします。
[Boot Override Priority] ダイアログボックスが開きます。

ステップ 4 [Boot Override Priority] ダイアログボックスで、ブート元の仮想ドライブを選択します。

ステップ 5 [OK] 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 をリセットする必要はありません。 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のみ、この手順を実行することを推奨します。

（注） この操作によって、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は中断されます。

はじめる前に

- このタスクを実行するには、ユーザ権限または admin 権限を使用してログインする必要があります。
- Cisco Flexible Flash がプラットフォームでサポートされている必要があります。

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Inventory] をクリックします。

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

ステップ 4 [Storage Adapters] テーブルで、FlexFlash コントローラをクリックします。
選択した FlexFlash コントローラのプロパティが、[Storage Adapters] 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 [Storage Card] タブ付きメニューで、[Controller Info] タブをクリックします。

ステップ 6 [Actions] 領域で [Reset Cisco Flex Flash] をクリックします。

ステップ 7 [OK] をクリックして確定します。

BIOS の設定

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、ユーザ権限または admin 権限を使用してログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [BIOS] をクリックします。

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

ステップ 4 [Configure BIOS Parameters] ダイアログボックスで、[Main] タブをクリックします。

ステップ 5 変更の保存後にサーバをリブートするかどうかを指定します。
[Save Changes] をクリックすると変更が自動的に適用されるようにするには、[Reboot Host Immediately]チェックボックスをオンにします。 CIMC によってすぐにサーバがリブートされ、変更が適用されます。

後で変更を適用するには、[Reboot Host Immediately] チェックボックスをオフにします。 CIMC によって変更が保存され、次回のサーバ リブート時に適用されます。

（注） 既存の BIOS パラメータ変更が保留中の場合は、[Save Changes] をクリックすると、保存されている値が自動的に現在の設定で上書きされます。

ステップ 6 [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、次のいずれかを参照してください。

- C200 および C210 サーバの主要な BIOS パラメータ，（169 ページ）
- C250 サーバの主要な BIOS パラメータ，（186 ページ）
- C260 サーバの主要な BIOS パラメータ，（201 ページ）
- C460 サーバの主要な BIOS パラメータ，（217 ページ）

ステップ 7 （任意） パラメータをリセットするか、[Configure BIOS Parameters] ダイアログボックスの一番下にあるボタンを使用してデフォルト値に戻すことができます。
使用可能なオプションは次のとおりです。

名前	説明
[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。 [Reboot Host Immediately] チェックボックスがオンの場合、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、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。
[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を最初に開いたときに有効であった設定に戻します。
[Restore Defaults] ボタン	3 つのタブすべての BIOS パラメータをデフォルト設定に設定します。
[Cancel] ボタン	変更しないで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、表示しているタブのパラメータだけではなく、使用可能なすべてのタブにあるすべての BIOS パラメータに影響します。

ステップ 8 [Save Changes] をクリックします。

高度な BIOS の設定

（注） 設置されているハードウェアによっては、この項で説明する一部の設定オプションは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、ユーザ権限または admin 権限を使用してログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [BIOS] をクリックします。

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

ステップ 4 [Configure BIOS Parameters] ダイアログボックスで、[Advanced] タブをクリックします。

ステップ 5 変更の保存後にサーバをリブートするかどうかを指定します。
[Save Changes] をクリックすると変更が自動的に適用されるようにするには、[Reboot Host Immediately] チェックボックスをオンにします。 CIMC によってすぐにサーバがリブートされ、変更が適用されます。

後で変更を適用するには、[Reboot Host Immediately] チェックボックスをオフにします。 CIMC によって変更が保存され、次回のサーバ リブート時に適用されます。

（注） 既存の BIOS パラメータ変更が保留中の場合は、[Save Changes] をクリックすると、保存されている値が自動的に現在の設定で上書きされます。

ステップ 6 [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、次のいずれかを参照してください。

- C200 および C210 サーバの高度な BIOS パラメータ，（170 ページ）
- C250 サーバの高度な BIOS パラメータ，（187 ページ）
- C260 サーバの高度な BIOS パラメータ，（202 ページ）
- C460 サーバの高度な BIOS パラメータ，（218 ページ）

ステップ 7 （任意） パラメータをリセットするか、[Configure BIOS Parameters] ダイアログボックスの一番下にあるボタンを使用してデフォルト値に戻すことができます。
使用可能なオプションは次のとおりです。

名前	説明
[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。 [Reboot Host Immediately] チェックボックスがオンの場合、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、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	説明
[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を最初に開いたときに有効であった設定に戻します。
[Restore Defaults] ボタン	3 つのタブすべての BIOS パラメータをデフォルト設定に設定します。
[Cancel] ボタン	変更しないで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、表示しているタブのパラメータだけではなく、使用可能なすべてのタブにあるすべての BIOS パラメータに影響します。

ステップ 8 [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、ユーザ権限または admin 権限を使用してログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [BIOS] をクリックします。

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

ステップ 4 [Configure BIOS Parameters] ダイアログボックスで、[Server Management] タブをクリックします。

ステップ 5 変更の保存後にサーバをリブートするかどうかを指定します。
[Save Changes] をクリックすると変更が自動的に適用されるようにするには、[Reboot Host Immediately] チェックボックスをオンにします。 CIMC によってすぐにサーバがリブートされ、変更が適用されます。

後で変更を適用するには、[Reboot Host Immediately] チェックボックスをオフにします。 CIMC によって変更が保存され、次回のサーバ リブート時に適用されます。

（注） 既存の BIOS パラメータ変更が保留中の場合は、[Save Changes] をクリックすると、保存されている値が自動的に現在の設定で上書きされます。

ステップ 6 [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、次のいずれかを参照してください。

- C200 および C210 サーバのサーバ管理 BIOS パラメータ，（183 ページ）
- C250 サーバのサーバ管理 BIOS パラメータ，（198 ページ）
- C260 サーバのサーバ管理 BIOS パラメータ，（213 ページ）
- C460 サーバのサーバ管理 BIOS パラメータ，（229 ページ）

ステップ 7 （任意） パラメータをリセットするか、[Configure BIOS Parameters] ダイアログボックスの一番下にあるボタンを使用してデフォルト値に戻すことができます。
使用可能なオプションは次のとおりです。

名前	説明
[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。 [Reboot Host Immediately] チェックボックスがオンの場合、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、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。
[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を最初に開いたときに有効であった設定に戻します。
[Restore Defaults] ボタン	3 つのタブすべての BIOS パラメータをデフォルト設定に設定します。
[Cancel] ボタン	変更しないで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、表示しているタブのパラメータだけではなく、使用可能なすべてのタブにあるすべての BIOS パラメータに影響します。

ステップ 8 [Save Changes] をクリックします。

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，37 ページ
- CIMC 情報の表示，38 ページ
- CPU のプロパティの表示，39 ページ
- メモリのプロパティの表示，39 ページ
- 電源のプロパティの表示，42 ページ
- ストレージのプロパティの表示，42 ページ
- PCI アダプタのプロパティの表示，43 ページ

サーバのプロパティの表示

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Summary] をクリックします。

ステップ 3 [Server Summary] ペインの [Server Properties] 領域で、次の情報を確認します。

名前	説明
[Product Name] フィールド	サーバのモデル名。
[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。

名前	説明
[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。
[Description] フィールド	サーバのユーザ定義の説明。

CIMC 情報の表示

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Summary] をクリックします。

ステップ 3 [Server Summary] ペインの [Cisco Integrated Management Controller (CIMC) Information] 領域で、次の情報を確認します。

名前	説明
[Hostname] フィールド	CIMC のユーザ定義のホスト名。
[IP Address] フィールド	CIMC の IP アドレス。
[MAC Address] フィールド	CIMC 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。
[Firmware Version] フィールド	現在の CIMC ファームウェアのバージョン。
[Current Time] フィールド	CIMC クロックが示している現在の日時。 （注） CIMCは、サーバBIOSから現在の日時を取得します。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。

CPU のプロパティの表示

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Inventory] をクリックします。

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

ステップ 4 各 CPU で次の情報を確認します。

名前	説明
[Socket Name] フィールド	CPU が装着されているソケット
[Vendor] フィールド	CPU のベンダー
[Status] フィールド	CPU のステータス。
[Family] フィールド	この CPU が属すファミリ。
[Speed] フィールド	CPU の速度（メガヘルツ単位）。
[Version] フィールド	CPU のバージョン
[Number of Cores] フィールド	CPU のコアの数
[Signature] フィールド	CPU のシグニチャ情報。
[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 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Inventory] をクリックします。

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

ステップ 4 [Memory 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	説明
[Memory Speed] フィールド	メモリ速度（メガヘルツ単位）。
[Failed Memory] フィールド	現在障害のあるメモリの量（メガヘルツ単位）。
[Total Memory] フィールド	すべてのDIMMが完全に機能する場合にサーバで使用できるメモリの合計量。
[Ignored Memory] フィールド	現在使用できないメモリの量（メガヘルツ単位）。
[Effective Memory] フィールド	現在サーバで実際に使用できるメモリの量。
[Number of Ignored DIMMs] フィールド	サーバがアクセスできない DIMM の数。
[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。
[Number of Failed DIMMs] フィールド	障害が発生して使用できない DIMM の数。
[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。
[Memory Configuration] フィールド	現在のメモリ構成。 次のいずれかになります。 • [Maximum Performance]：メモリ パフォーマンスが自動的に最適化されます。 • [Mirroring]：データの 2 つの同一コピーがメモリに保持されます。 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。 • [Sparing]：一部のメモリがDIMM障害時の使用のために予約されます。 障害が発生すると、DIMMはオフラインになり、予約済みメモリと交換されます。 このオプションを使用した場合、ミラーリングよりも冗長性が低くなりますが、サーバで実行されているプログラムに使用できるメモリの量は多くなります。

ステップ 5 [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	説明
[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
[Capacity] カラム	DIMM のサイズ。
[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）。
[Channel Type] カラム	メモリ チャネルのタイプ。
[Memory Type Detail] カラム	デバイスで使用されるメモリのタイプ。
[Bank Locator] カラム	メモリ バンク内の DIMM の位置。
[Manufacturer] カラム	製造元のベンダー ID。 次のいずれかになります。 • [0x2C00]：Micron Technology, Inc. • [0x5105]：Qimonda AG i. In. • [0x802C]：Micron Technology, Inc. • [0x80AD]：Hynix Semiconductor Inc. • [0x80CE]：Samsung Electronics, Inc. • [0x8551]：Qimonda AG i. In. • [0xAD00]：Hynix Semiconductor Inc. • [0xCE00]：Samsung Electronics, Inc.
[Serial Number] カラム	DIMM のシリアル番号。
[Asset Tag] カラム	DIMM に関連付けられている資産タグ（ある場合）。
[Part Number] カラム	ベンダーによって割り当てられている DIMM の製品番号。
[Visibility] カラム	DIMM がサーバで使用可能かどうか。
[Operability] カラム	DIMM が現在正常に動作しているかどうか。
[Data Width] カラム	DIMM でサポートされるデータの量（ビット単位）。

電源のプロパティの表示

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Inventory] をクリックします。

ステップ 3 [Inventory] ペインの [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	説明
[Device ID] カラム	電源装置ユニットの ID。
[Input] カラム	電源装置への入力（ワット単位）。
[Max Output] カラム	電源装置からの最大出力（ワット単位）。
[FW Version] カラム	電源装置のファームウェア バージョン。
[Product ID] カラム	ベンダーによって割り当てられている電源装置の製品 ID。

ストレージのプロパティの表示

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Inventory] をクリックします。

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

ステップ 4 [Storage Adapters] 領域で、使用可能なアダプタ カードに関する情報を確認します。
この領域には、CIMC で管理できるサーバ上のすべての MegaRAID と Cisco Flexible Flash コントローラのリストがテーブルで示されます。 特定のストレージ デバイスの詳細を表示するには、テーブルでデバイスを選択して下のタブに情報を表示します。

特定のストレージ デバイスがこのタブに表示されない場合は、そのデバイスを CIMC で管理できません。 サポートされていないデバイスのステータスを表示するには、そのデバイスのマニュアルを参照してください。

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。

ステップ 5　[Storage Adapters] 領域で、行をクリックして、アダプタの詳細なプロパティを表示します。
選択したストレージ アダプタのプロパティが、[Storage Adapters] 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　[Controller Info] タブを選択して、情報を確認します。
このタブには、MegaRAID コントローラまたは [Storage Adapters] テーブルで選択した Cisco Flexible Flash コントローラに関する情報が表示されます。

（注）　このタブおよび以降のタブに表示されるフィールドの詳細については、UCSM GUI で提供されるオンライン ヘルプを参照してください。

ステップ 7　[Physical Drive Info] タブを選択して、情報を確認します。
このタブには、[Storage Adapters] テーブルで選択したコントローラの次の情報が表示されます。

- ドライブの一般情報
- 識別情報
- ドライブの状態

ステップ 8　[Virtual Drive Info] タブを選択して、情報を確認します。
このタブには、[Storage Adapters] テーブルで選択したコントローラの次の情報が表示されます。

- ドライブの一般情報
- RAID 情報
- 物理ドライブの情報

ステップ 9　[Battery Backup Unit] タブを選択して、情報を確認します。
このタブには、[Storage Adapters] テーブルで選択したコントローラ上のバックアップ バッテリに関する情報が表示されます。

（注）　[Storage Adapters] テーブルで Cisco Flexible Flash コントローラを選択した場合、このタブは適用されません。

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 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Inventory] をクリックします。

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

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

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

第 5 章

サーバのセンサーの表示

この章の内容は、次のとおりです。

- 障害の要約の表示，45 ページ
- 電源センサーの表示，46 ページ
- ファン センサーの表示，48 ページ
- 温度センサーの表示，49 ページ
- 電圧センサーの表示，50 ページ
- 電流センサーの表示，51 ページ
- LED センサーの表示，52 ページ
- ストレージ センサーの表示，52 ページ

障害の要約の表示

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Fault Summary] をクリックします。

ステップ 3 [Discrete Sensors] 領域で、次の情報を確認します。

名前	説明
[Sensor Name] カラム	センサーの名前。

名前	説明
[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。 • Critical • Non-Recoverable • Warning
[Reading] カラム	センサーの基本状態。

ステップ 4 [Threshold Sensors] 領域で、次の情報を確認します。

名前	説明
[Sensor Name] カラム	センサーの名前。
[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。 • Critical • Non-Recoverable • Warning
[Reading] カラム	センサーによって報告された値。
[Units] カラム	報告されたセンサー データの単位。
[Warning Threshold Min] カラム	Warning の最小しきい値。
[Warning Threshold Max] カラム	Warning の最大しきい値。
[Critical Threshold Min] カラム	Critical の最小しきい値。
[Critical Threshold Max] カラム	Critical の最大しきい値。

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 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Sensors] をクリックします。

ステップ 3 [Sensors] ペインの [Power Supply] タブをクリックします。

ステップ 4 [Properties] 領域で、[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 [Discrete Sensors] 領域で、次に示すサーバの統計情報を表示できます。

名前	説明
[Sensor Name] カラム	センサーの名前。
[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。 • Unknown • Informational • Normal • Warning • Critical • Non-Recoverable
[Reading] カラム	センサーの基本状態。

ステップ 6 [Threshold Sensors] 領域で、次に示すサーバの統計情報を表示できます。

名前	説明
[Sensor Name] カラム	センサーの名前。
[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。 • Unknown • Informational • Normal • Warning • Critical • Non-Recoverable
[Reading] カラム	現在の電力使用量（ワット単位）。

名前	説明
[Warning Threshold Min] カラム	Warning の最小しきい値。
[Warning Threshold Max] カラム	Warning の最大しきい値。
[Critical Threshold Min] カラム	Critical の最小しきい値。
[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 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Sensors] をクリックします。

ステップ 3 [Sensors] ペインの [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	説明
[Sensor Name] カラム	センサーの名前。
[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。 • Unknown • Informational • Normal • Warning • Critical • Non-Recoverable
[Speed] カラム	ファンの速度（RPM 単位）。
[Warning Threshold Min] カラム	Warning の最小しきい値。

名前	説明
[Warning Threshold Max] カラム	Warning の最大しきい値。
[Critical Threshold Min] カラム	Critical の最小しきい値。
[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 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Sensors] をクリックします。

ステップ 3 [Sensors] ペインの [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	説明
[Sensor Name] カラム	センサーの名前。
[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。 • Unknown • Informational • Normal • Warning • Critical • Non-Recoverable
[Temperature] カラム	現在の温度（摂氏単位）。
[Warning Threshold Min] カラム	Warning の最小しきい値。
[Warning Threshold Max] カラム	Warning の最大しきい値。

名前	説明
[Critical Threshold Min] カラム	Critical の最小しきい値。
[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 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Sensors] をクリックします。

ステップ 3 [Sensors] ペインの [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	説明
[Sensor Name] カラム	センサーの名前。
[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。 • Unknown • Informational • Normal • Warning • Critical • Non-Recoverable
[Voltage] カラム	現在の電圧（ボルト単位）。
[Warning Threshold Min] カラム	Warning の最小しきい値。
[Warning Threshold Max] カラム	Warning の最大しきい値。
[Critical Threshold Min] カラム	Critical の最小しきい値。

名前	説明
[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 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Sensors] をクリックします。

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

ステップ 4 [Current] タブで、次の電流関連の統計情報を表示します。

名前	説明
[Sensor Name] カラム	センサーの名前。
[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。 • Unknown • Informational • Normal • Warning • Critical • Non-Recoverable
[Current] カラム	電流（アンペア単位）。
[Warning Threshold Min] カラム	Warning の最小しきい値。
[Warning Threshold Max] カラム	Warning の最大しきい値。
[Critical Threshold Min] カラム	Critical の最小しきい値。
[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 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Sensors] をクリックします。

ステップ 3 [Sensors] ペインの [LEDs] 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	説明
[Sensor Name] カラム	センサーの名前。
[LED State] カラム	LED がオンか点滅かオフか。
[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のタイプのハードウェア 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 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Sensors] をクリックします。

ステップ 3 [Sensors] ペインの [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	説明
[Name] カラム	ストレージ デバイスの名前。
[Status] カラム	ストレージ デバイスのステータスに関する簡単な説明。

第 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。

- Serial over LAN の設定，55 ページ
- 仮想メディアの設定，56 ページ
- KVM コンソール，57 ページ
- 仮想 KVM の設定，58 ページ

Serial over LAN の設定

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

はじめる前に

Serial over LAN を設定するには、管理者権限のあるユーザでログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Remote Presence] をクリックします。

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

名前	説明
[Enabled] チェックボックス	オンにすると、このサーバで Serial over LAN がイネーブルになります。

名前	説明
[Baud Rate] ドロップダウン リスト	システムが Serial over LAN 通信に使用するボー レート。 次のいずれかを選択できます。 • 9600 bps • 19.2 kbps • 38.4 kbps • 57.6 kbps • 115.2 kbps

ステップ 5 [Save Changes] をクリックします。

仮想メディアの設定

はじめる前に

仮想メディアを設定するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Remote Presence] をクリックします。

ステップ 3 [Remote Presence] ペインの [Virtual Media] タブをクリックします。

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

名前	説明
[Enabled] 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。
[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。
[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。

ステップ 5 [Save Changes] をクリックします。

KVM コンソール

KVMコンソールはCIMC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 上の 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。 この場合は、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] セクションで [Do not save encrypted pages to disk] の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。

（注） KVM コンソールは、GUI からのみ操作します。 KVM コンソールを起動するには、『*Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide*』の手順を参照してください。

仮想 KVM の設定

はじめる前に

仮想 KVM を設定するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Remote Presence] をクリックします。

ステップ 3 [Remote Presence] ペインの [Virtual KVM] タブをクリックします。

ステップ 4 [Virtual KVM] タブで、次のフィールドに値を入力します。

名前	説明
[Enabled] 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、CIMC 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。
[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。
[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。
[Remote Port] フィールド	KVM 通信に使用するポート。
[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。
[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 [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 [Navigation] ペインの [Server] タブをクリックします。
ステップ 2 [Server] タブの [Remote Presence] をクリックします。
ステップ 3 [Remote Presence] ペインの [Virtual KVM] タブをクリックします。
ステップ 4 [Virtual KVM] タブで、 [Enabled] チェックボックスをオンにします。
ステップ 5 [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 [Navigation] ペインの [Server] タブをクリックします。
ステップ 2 [Server] タブの [Remote Presence] をクリックします。
ステップ 3 [Remote Presence] ペインの [Virtual KVM] タブをクリックします。
ステップ 4 [Virtual KVM] タブで、 [Enabled] チェックボックスをオフにします。
ステップ 5 [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。

- ローカル ユーザの設定，61 ページ
- Active Directory，62 ページ
- ユーザ セッションの表示，66 ページ

ローカル ユーザの設定

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 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [User Management] をクリックします。

ステップ 3 [User Management] ペインの [Local User] 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 [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	説明
[ID] カラム	ユーザの固有識別情報。
[Enabled] チェックボックス	オンにすると、ユーザは CIMC でイネーブルになります。
[Username] カラム	ユーザのユーザ名。

名前	説明
[Role] カラム	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。 • [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。 • [user]：このロールのユーザは、次のタスクを実行できます。 ◦すべての情報を表示する ◦電源のオン、電源再投入、電源のオフなどの電力制御オプションを管理する ◦KVM コンソールと仮想メディアを起動する ◦すべてのログをクリアする ◦ロケータ LED を切り替える • [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。

ステップ 6 パスワード情報を入力します。

ステップ 7 [Save Changes] をクリックします。

Active Directory

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。CIMC は、Active Directory の Kerberos ベースの認証サービスを利用します。

CIMC で Active Directory をイネーブルにすると、ローカル ユーザ データベースで見つからないユーザ アカウントについて、ユーザ認証とロール許可は Active Directory によって実行されます。

[Active Directory Properties] 領域の [Enable Encryption] チェックボックスをオンにすることで、サーバでの Active Directory の設定で暗号化をイネーブルにすることで、サーバに Active Directory への送信データを暗号化するよう要求できます。

Active Directory サーバの設定

CIMC を設定して、Active Directory をユーザの認証と認可に使用できます。 Active Directory を使用するには、CIMC のユーザ ロールとロケールを保持する属性を使用してユーザを設定します。CIMC 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、Active Directory 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 属性のような新規のカスタム属性を追加できます。 Active Directory 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。

Active Directory サーバで次の手順が実行します。

（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、CIMC 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。

手順

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

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

プロパティ	値
Common Name	CiscoAVPair
LDAP Display Name	CiscoAVPair
Unique X500 Object ID	1.3.6.1.4.1.9.287247.1
Description	CiscoAVPair
Syntax	Case Sensitive String

ステップ 3 Active Directory 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 CIMC 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。

ロール	CiscoAVPair 属性値
admin	shell:roles="admin"

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

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

次の作業

CIMC を使用して Active Directory を設定します。

CIMC での Active Directory 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 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [User Management] をクリックします。

ステップ 3 [User Management] ペインの [Active Directory] タブをクリックします。

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

名前	説明
[Enabled] チェックボックス	オンにすると、ローカル ユーザ データベースで見つからないユーザ アカウントのユーザ認証とロール許可が Active Directory によって実行されます。 このチェックボックスをオンにすると、このセクション内の残りのフィールドがイネーブルになります。
[Domain Controller] フィールド	CIMC で LDAP データベースへのアクセスに使用できる LDAP ドメイン コントローラを最大 3 つ指定できます。 CIMC は、このタブで指定された順に IP アドレスを使用してデータベースに接続しようとします。

名前	説明
[Timeout] フィールド	LDAP 検索操作がタイムアウトするまで CIMC が待機する秒数。 検索操作がタイムアウトすると、CIMC は、このタブにリストされている次のドメイン コントローラまたはグローバル カタログに接続しようとします（使用可能な場合）。
[Enable Encryption] チェックボックス	オンにすると、サーバは Active Directory に送信するすべての情報を暗号化します。
[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。 少なくとも 1 つのグローバル カタログ サーバ アドレスを指定した場合を除き、このフィールドは必須です。
[Attributes] フィールド	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 属性は、次の属性 ID である必要があります。 CiscoAvPair （注） このプロパティを指定しない場合、ユーザ アクセスは read-only に制限されます。
[Global Catalog] フィールド	グローバル カタログを使用すると、ユーザが存在するドメインにかかわらず、CIMC で Active Directory からユーザを検索できます。 3 つの [Global Catalog] フィールドそれぞれに、グローバル カタログの IP アドレスまたは完全修飾ドメイン名（FQDN）を入力できます。 CIMC は、このタブで指定された順に IP アドレスまたは FQDN を使用してカタログにアクセスしようとします。

ステップ 5 （任意） [Active Directory Groups] 領域で、次のプロパティを更新します。

名前	説明
[LDAP Group Authorization] チェックボックス	オンにすると、ローカル ユーザ データベースに見つからないユーザまたは Active Directory で CIMC の使用が個別に許可されていないユーザに対するユーザ認証がグループ レベルで実行されます。 このチェックボックスをオンにすると、[Configure Group] ボタンがイネーブルになります。

名前	説明
[Group Name] カラム	サーバへのアクセスを許可された Active Directory データベース内のグループの名前。
[Group Domain] カラム	グループが存在する必要がある Active Directory ドメイン。
[Role] カラム	この Active Directory グループ内のすべてのユーザに割り当てられるロール。 次のいずれかになります。 • [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。 • [user]：このロールのユーザは、次のタスクを実行できます。 ◦ すべての情報を表示する ◦ 電源のオン、電源再投入、電源のオフなどの電力制御オプションを管理する ◦ KVM コンソールと仮想メディアを起動する ◦ すべてのログをクリアする ◦ ロケータ LED を切り替える • [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。

ステップ 6 [Save Changes] 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 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [User Management] をクリックします。

ステップ 3 [User Management] ペインの [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	説明
[Session ID] カラム	セッションの固有識別情報。
[Username] カラム	ユーザのユーザ名。
[IP Address] カラム	ユーザがサーバにアクセスした IP アドレス。
[Type] カラム	ユーザがサーバにアクセスした方法。
[Action] カラム	ユーザ アカウントに admin ユーザ ロールが割り当てられ、関連付けられているユーザ セッションを強制的に終了できる場合は、このカラムに [Terminate] と表示されます。 それ以外の場合は、N/A と表示されます。 （注） このタブから現在のセッションを終了することはできません。

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 の設定，69 ページ
- 共通プロパティの設定，72 ページ
- IPv4 の設定，72 ページ
- VLAN への接続，73 ページ
- ネットワーク セキュリティ設定，74 ページ

サーバ NIC の設定

サーバの NIC

CIMC への接続には、2 種類の NIC モードを使用できます。 一方のモードでは、プラットフォームに応じて、active-active または active-standby の冗長化モードを選択することもできます。

NIC モード

[NIC Properties] 領域の [NIC Mode] ドロップダウン リストでは、CIMC に到達できるポートを指定します。 プラットフォームに応じて、次のモード オプションを使用できます。

CIMC ネットワークの設定により、CIMC に到達できるポートが決定します。 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。

- [Cisco Card]：CIMC への接続は、搭載されたアダプタ カードを経由して使用できます。
- [Dedicated]：CIMC への接続は、管理イーサネット ポートを経由して使用できます。
- [Shared LOM]：CIMC への接続は、LAN On Motherboard（LOM; マザーボードのオンボード LAN）イーサネット ホスト ポートを経由した場合だけ使用できます。 一部のプラットフォームでは、[10 Gigabit Ethernet LOM] オプションを使用できます。

（注） shared_lom モードでは、すべてのホスト ポートが同じサブネットに属している必要があります。

- Shipping（サポートされている場合）：CIMC への接続は、制限された出荷時デフォルト設定を使用して、管理イーサネット ポートを経由して使用できます。

（注） shipping モードは、CIMC への初期接続の目的だけに用意されています。 運用時には別のモードを設定します。

NIC 冗長化

[NIC Properties] 領域の [NIC Redundancy] ドロップダウン リストでは、NIC 冗長化の処理方法を指定します。

CIMC ネットワーク冗長化の設定により、NIC 冗長化の処理方法が決定します。

- [None]：冗長化は使用できません。
- [Active-Active]：すべてのイーサネット ポートが同時に動作します。 このモードは、CIMC への複数のパスを提供します。
- [Active-Standby]：1 つのポートから別のポートにフェールオーバーします。

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。 使用できるモードについては、サーバのサーバ インストレーションおよびサービス ガイドを参照してください。 このガイドは http://www.cisco.com/go/unifiedcomputing/c-series-doc の『*Cisco UCS C-Series Servers Documentation Roadmap*』から入手できます。

サーバ NIC の設定

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

はじめる前に

NIC を設定するには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Network] をクリックします。

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

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

名前	説明
[NIC Mode] ドロップダウン リスト	NIC モード。 次のいずれかになります。 • [Dedicated]：CIMC へのアクセスに管理ポートを使用します。 • [Shared LOM]：CIMC へのアクセスに LAN On Motherboard（LOM; マザーボードのオンボード LAN）ポートを使用します。 • [Shared LOM 10G]：CIMC へのアクセスに 10 G ポートを使用します。 • [Cisco Card]：CIMC へのアクセスにアダプタ カードのポートを使用します。 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。 • [Shipping]：すべてのオプションにアウトオブザボックスのデフォルトを使用します。 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。
[NIC Redundancy] ドロップダウン リスト	NIC 冗長化オプションは、[NIC Mode] ドロップダウン リストで選択されているモードおよび使用しているサーバのモデルに依存します。 ある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。 使用可能なオプションは次のとおりです。 • [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。 • [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。 これにより、スループットが増加し、CIMC への複数のパスが提供されます。 • [active-standby]：設定されている NIC モードに関連付けられたポートで障害が発生した場合、トラフィックは、その NIC モードに関連付けられている他のポートの 1 つにフェールオーバーします。 （注） このオプションを選択する場合は、設定されている NIC モードに関連付けられたすべてのポートが同じサブネットに接続され、どのポートが使用されてもトラフィックの安全が保証されるようにする必要があります。

名前	説明
[MAC Address] フィールド	[NIC Mode] フィールドで選択されている CIMC ネットワーク インターフェイスの MAC アドレス。

（注） 使用可能な NIC モードのオプションは、お使いのプラットフォームによって異なります。

Shared LOM 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。

ステップ 5 [Save Changes] をクリックします。

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 [Navigation] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブの [Network] をクリックします。
ステップ 3 [Network] ペインの [Network Settings] タブをクリックします。
ステップ 4 [Hostname] フィールドに、ホストの名前を入力します。
ステップ 5 [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 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Network] をクリックします。

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

ステップ 4 [IPv4 Properties] 領域で、次のプロパティを更新します。

名前	説明
[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。
[Use DHCP] チェックボックス	オンにすると、CIMC は DHCP を使用します。
[IP Address] フィールド	CIMC の IP アドレス。
[Subnet Mask] フィールド	IP アドレスのサブネット マスク。
[Gateway] フィールド	IP アドレスのゲートウェイ。
[Obtain DNS Server Addresses from DHCP] チェックボックス	オンにすると、CIMC は DNS サーバ アドレスを DHCP から取得します。
[Preferred DNS Server] フィールド	プライマリ DNS サーバの IP アドレス。
[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 [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 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Network] をクリックします。

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

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

名前	説明
[Enable VLAN] チェックボックス	オンにすると、CIMC は仮想 LAN に接続されます。
[VLAN ID] フィールド	VLAN ID。
[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 [Save Changes] をクリックします。

ネットワーク セキュリティ設定

ネットワーク セキュリティ

CIMC 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、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効果的に禁止します。

禁止 IP の設定は、一般的に、Denial of Service（DoS; サービス拒絶）攻撃から保護するために使用されます。 CIMC 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 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Network] をクリックします。

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

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

名前	説明
[Enable IP Blocking] チェックボックス	このチェックボックスをオンにすると、IP ブロッキングがイネーブルになります。
[IP 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失敗は、[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 の範囲の整数を入力します。
[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 の範囲の整数を入力します。
[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 の範囲の整数を入力します。

ステップ 5 [Save Changes] 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，77 ページ
- ネットワーク アダプタのプロパティの表示，78 ページ
- アダプタのプロパティの設定，81 ページ
- vHBA の管理，83 ページ
- vNIC の管理，97 ページ
- VM FEX の管理，110 ページ
- アダプタ構成のバックアップと復元，115 ページ
- アダプタ ファームウェアの管理，117 ページ

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搭載されてい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 アダプタは、I/O 統合および仮想化のサポートのオプションを提供するために搭載できます。 次に、使用可能なアダプタを示します。

- 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

Cisco UCS P81E 仮想インターフェイス カードは、仮想化環境、物理的な環境でモビリティの向上を目指す組織、NIC、HBA、ケーブル接続、スイッチの削減によるコストの削減と管理面での負

荷の削減を求めるデータセンターに最適化されています。 この Fibre Channel over Ethernet（FCoE）PCIe カードには、次のような利点があります。

- ジャストインタイムのプロビジョニングを使用して、仮想化環境または非仮想化環境で、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 アダプタをプロビジョニングできます。システムに大きな柔軟性がもたらされ、複数の物理アダプタの統合が可能になります。
- 仮想化の徹底的なサポートが提供されます。Cisco VN-Link テクノロジーのハードウェアベースの実装およびパススルー スイッチングが含まれます。
- ネットワーク ポリシーおよびセキュリティの可視性とポータビリティを仮想マシンにまで提供することによって、システムのセキュリティと管理性が向上します。

仮想インターフェイス カードによって、親ファブリック インターコネクトへの Cisco VN-Link 接続が行われます。これにより、仮想リンクは仮想マシンの仮想 NIC をインターコネクトの仮想インターフェイスに接続できます。 Cisco Unified Computing System 環境では、仮想マシンがシステム内のサーバ間を移動したときに、仮想リンクを管理し、ネットワーク プロファイルを適用し、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。

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。
- Cisco UCS P81E 仮想インターフェイス カードをシャーシに取り付けて、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 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Inventory] をクリックします。

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

ステップ 4 [Adapter Cards] 領域で、表内のアダプタをクリックしてプロパティを表示します。
選択したアダプタのリソースが、[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 [Adapter Cards] 領域で、搭載されているアダプタに関する次の情報を確認します。

名前	説明
[PCI Slot] カラム	アダプタが装着されている PCI スロット。
[Product Name] カラム	アダプタの製品名。
[Serial Number] カラム	アダプタのシリアル番号。

名前	説明
[Product ID] カラム	アダプタの製品 ID。
[Vendor] カラム	アダプタのベンダー。
[CIMC Management Enabled] カラム	アダプタで CIMC を管理できるかどうか。 この機能は、取り付けられているアダプタのタイプとその設定方法に依存します。詳細については、使用しているサーバのタイプのハードウェア 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 [Adapter Cards] 領域の下のタブ付きメニューで、[General] タブをクリックします。

ステップ 7 [Adapter Card Properties] 領域で、アダプタに関する次の情報を確認します。

名前	説明
[PCI Slot] フィールド	アダプタが装着されている PCI スロット。
[Vendor] フィールド	アダプタのベンダー。
[Product Name] フィールド	アダプタの製品名。
[Product ID] フィールド	アダプタの製品 ID。
[Serial Number] フィールド	アダプタのシリアル番号。
[Version ID] フィールド	アダプタのバージョン ID。
[Hardware Revision] フィールド	アダプタのハードウェア リビジョン。
[CIMC Management Enabled] フィールド	このフィールドに [yes] が表示される場合、アダプタは Cisco Card モードで動作し、CIMC 管理トラフィックをサーバ CIMC に渡します。
[Configuration Pending] フィールド	このフィールドに [yes] が表示される場合、アダプタ設定が CIMC で変更されていますが、これらの変更はホスト オペレーティング システムに伝達されていません。 変更をアクティブ化するには、管理者がアダプタをリブートする必要があります。
[Description] フィールド	アダプタのユーザ定義の説明（ある場合）。
[FIP Mode] フィールド	FCoE Initialization Protocol（FIP）モードをイネーブルにするかどうか。 FIP モードの場合、アダプタは現在の FCoE 標準と互換性があります。

名前	説明
[NIV Mode] フィールド	ネットワーク インターフェイスの仮想化（NIV）をイネーブルにするかどうか。 NIV モードがイネーブルの場合： • vNIC と vHBA を特定のチャネルに割り当てることができます • vNIC と vHBA をポート プロファイルに関連付けることができます • 通信上の問題が発生した場合、vNIC は別の vNIC にフェールオーバーできます

ステップ 8 [External Ethernet Interfaces] 領域で、アダプタに関する次の情報を確認します。

名前	説明
[ID] カラム	アップリンク ポートの ID。
[MAC Address] カラム	アップリンク ポートの MAC アドレス。
[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 • Link Up • Link Down • SFP ID Error • SFP Not Installed • SFP Security Check Failed • Unsupported SFP
[Encap] カラム	ネットワーク インターフェイスの仮想化（NIV）をサポートするために仮想ネットワーク タグ（VNTag）に追加される属性。

ステップ 9 [Firmware] 領域で、アダプタに関する次の情報を確認します。

名前	説明
[Running Version] フィールド	現在アクティブなファームウェア バージョン。

名前	説明
[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（ある場合）。バックアップ バージョンは現在実行されていません。アクティブ化するには、管理者が [Actions] 領域の [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 バージョンが削除され、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必要がある場合は、手動で新しいファームウェアをアクティブ化する必要があります。
[Startup Version] フィールド	アダプタを次にリブートしたときにアクティブになるファームウェア バージョン。
[Status] フィールド	このアダプタで実行された最後のファームウェア アクティベーションのステータス。 （注） アダプタをリブートするたびにステータスがリセットされます。

次の作業

仮想 NIC、VM FEX、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, （98 ページ）
- 仮想 FEX のプロパティの表示, （110 ページ）
- vHBA のプロパティの表示, （83 ページ）

アダプタのプロパティの設定

はじめる前に

- このタスクを実行するには、ユーザ権限または admin 権限を使用してログインする必要があります。
- Cisco UCS P81E 仮想インターフェイス カードをシャーシに取り付けて、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 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Inventory] をクリックします。

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

ステップ 4 [Adapter Cards] 領域で、アダプタ カードを選択します。
サーバの電源をオンにすると、選択したアダプタ カードのリソースが [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 [Adapter Cards] 領域の下のタブ付きメニューで、[General] タブをクリックします。

ステップ 6 [General] タブの [Actions] 領域で、[Set Adapter Properties] をクリックします。
[Modify Adapter Properties] ダイアログボックスが開きます。

ステップ 7 [Modify Adapter Properties] ダイアログボックスで、次のフィールドを更新します。

名前	説明
[Description] フィールド	アダプタのユーザ定義の説明。 1 ～ 63 文字を入力できます。
[Enable FIP Mode] チェックボックス	オンにすると、FCoE Initialization Protocol（FIP）モードがイネーブルになります。 FIP モードの場合、アダプタは現在の FCoE 標準と互換性があります。 （注） 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、このオプションを使用することを推奨します。
[Enable NIV Mode] チェックボックス	オンにすると、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ります。 NIV モードがイネーブルの場合： • vNIC と vHBA を特定のチャネルに割り当てることができます • vNIC と vHBA をポート プロファイルに関連付けることができます • 通信上の問題が発生した場合、vNIC は別の vNIC にフェールオーバーできます
[Number of VM FEX Interfaces] フィールド	CIMC で作成する VM FEX インターフェイスの数。 0 ～ 112 の整数を入力します。 （注） このオプションでは NIV モードが必要です。

ステップ 8 [Save Changes] をクリックします。

vHBA の管理

vHBA の管理上の注意事項

vHBA を管理するときは、次の注意事項および制約事項を考慮してください。

- Cisco UCS P81E 仮想インターフェイス カードには、2 つの vHBA（fc0 および fc1）があります。 このアダプタ カードでは最大 16 個の vHBA を追加作成できます。

（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である場合は、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 カードを使用する場合は、vHBA を FCoE VLAN に関連付けている必要があります。 VLAN を割り当てるには、vHBA のプロパティの変更, （88 ページ）vHBA のプロパティの変更の手順に従います。
- 設定の変更後、設定を反映するには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 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Inventory] をクリックします。

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

ステップ 4 [Adapter Cards] 領域で、アダプタ カードを選択します。
サーバの電源をオンにすると、選択したアダプタ カードのリソースが [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 [Adapter Cards] 領域の下のタブ付きメニューで、[vHBAs] タブをクリックします。

ステップ 6 [Host Fibre Channel Interfaces] 領域で、テーブルから vHBA を選択します。

ステップ 7 [Properties] をクリックして、[vHBA Properties] ダイアログボックスを開きます。

ステップ 8 [General] 領域で、次のフィールドの情報を確認します。

名前	説明
[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。
[World Wide Node Name] フィールド	vHBA に関連付けられている WWNN。 WWNN を自動的に生成するには、[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。
[World Wide Port Name] フィールド	vHBA に関連付けられている WWPN。 WWPN を自動的に生成するには、[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 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。
[Enable Persistent LUN Binding] チェックボックス	オンにすると、LUN ID の関連付けが手動でクリアされるまでメモリに保持されます。
[Uplink Port] フィールド	vHBA に関連付けられているアップリンク 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 Address] フィールド	vHBA に関連付けられている MAC アドレス。 MAC アドレスを自動的に生成するには、[AUTO] を選択します。 アドレスを指定するには、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 MAC アドレスを入力します。
[Default VLAN] フィールド	この vHBA のデフォルト VLAN がない場合は、[NONE] をクリックします。 それ以外の場合は、2 つ目のオプション ボタンをクリックし、フィールドに 1 ～ 4094 の VLAN ID を入力します。
[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 は最低プライオリティを表し、6 は最高プライオリティを表します。 （注） このオプションは、NIV モードでは使用できません。

名前	説明
[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 のデータ レートを制限しない場合は、[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、NIV モードでは使用できません。
[PCIe Device Order] フィールド	この vHBA が使用される順序。 順序を自動的に設定するには、[ANY] を選択します。 順序を指定するには、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）。エラーが発生したと見なす前にシステムが待機するミリ秒数。 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）。リソースを適切に割り当てることができないと見なす前にシステムが待機するミリ秒数。 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。
[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 の範囲の整数を入力します。
[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） このオプションでは NIV モードが必要です。
[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、このサーバの接続先スイッチに定義されているポート プロファイルが表示されます。 （注） このオプションでは NIV モードが必要です。

ステップ 9 [Error Recovery] 領域で、次のフィールドの情報を確認します。

名前	説明
[Enable FCP Error Recovery] チェックボックス	オンにすると、システムで FCP Sequence Level Error Recovery プロトコル（FC-TAPE）が使用されます。
[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。
[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。
[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 [Fibre Channel Interrupt] 領域で、次のフィールドの情報を確認します。

名前	説明
[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 だけ。 • [INTx]：PCI INTx 割り込み。

ステップ 11 [Fibre Channel Port] 領域で、次のフィールドの情報を確認します。

名前	説明
[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。
[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 [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	説明
[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するには、[INFINITE] オプション ボタンを選択します。 それ以外の場合は、2 つ目のオプション ボタンを選択し、対応するフィールドに整数を入力します。
[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 [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	説明
[PLOGI Retries] 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 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	説明
[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 Work 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 [Receive/Transmit Queues] 領域で、次のフィールドの情報を確認します。

名前	説明
[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。

名前	説明
[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 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Inventory] をクリックします。

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

ステップ 4 [Adapter Cards] 領域で、アダプタ カードを選択します。
サーバの電源をオンにすると、選択したアダプタ カードのリソースが [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 [Adapter Cards] 領域の下のタブ付きメニューで、[vHBAs] タブをクリックします。

ステップ 6 [Host Fibre Channel Interfaces] 領域で、テーブルから vHBA を選択します。

ステップ 7 [Properties] をクリックして、[vHBA Properties] ダイアログボックスを開きます。

ステップ 8 [General] 領域で、次のフィールドを更新します。

名前	説明
[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。
[World Wide Node Name] フィールド	vHBA に関連付けられている WWNN。 WWNN を自動的に生成するには、[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。
[World Wide Port Name] フィールド	vHBA に関連付けられている WWPN。 WWPN を自動的に生成するには、[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 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	説明
[Enable Persistent LUN Binding] チェックボックス	オンにすると、LUN ID の関連付けが手動でクリアされるまでメモリに保持されます。
[Uplink Port] フィールド	vHBA に関連付けられているアップリンク 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 Address] フィールド	vHBA に関連付けられている MAC アドレス。 MAC アドレスを自動的に生成するには、[AUTO] を選択します。 アドレスを指定するには、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 MAC アドレスを入力します。
[Default VLAN] フィールド	この vHBA のデフォルト VLAN がない場合は、[NONE] をクリックします。 それ以外の場合は、2 つ目のオプション ボタンをクリックし、フィールドに 1 ～ 4094 の VLAN ID を入力します。
[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 は最低プライオリティを表し、6 は最高プライオリティを表します。 （注） このオプションは、NIV モードでは使用できません。
[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 のデータ レートを制限しない場合は、[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、NIV モードでは使用できません。
[PCIe Device Order] フィールド	この vHBA が使用される順序。 順序を自動的に設定するには、[ANY] を選択します。 順序を指定するには、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）。エラーが発生したと見なす前にシステムが待機するミリ秒数。 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	説明
[RATOV] フィールド	リソース割り当てタイムアウト値（RATOV）。リソースを適切に割り当てることができないと見なす前にシステムが待機するミリ秒数。 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。
[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 の範囲の整数を入力します。
[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） このオプションでは NIV モードが必要です。
[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、このサーバの接続先スイッチに定義されているポート プロファイルが表示されます。 （注） このオプションでは NIV モードが必要です。

ステップ 9 [Error Recovery] 領域で、次のフィールドを更新します。

名前	説明
[Enable FCP Error Recovery] チェックボックス	オンにすると、システムで FCP Sequence Level Error Recovery プロトコル（FC-TAPE）が使用されます。
[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。
[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	説明
[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 [Fibre Channel Interrupt] 領域で、次のフィールドを更新します。

名前	説明
[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 だけ。 • [INTx]：PCI INTx 割り込み。

ステップ 11 [Fibre Channel Port] 領域で、次のフィールドを更新します。

名前	説明
[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。
[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 [Fibre Channel Port FLOGI] 領域で、次のフィールドを更新します。

名前	説明
[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するには、[INFINITE] オプション ボタンを選択します。 それ以外の場合は、2 つ目のオプション ボタンを選択し、対応するフィールドに整数を入力します。
[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 [Fibre Channel Port PLOGI] 領域で、次のフィールドを更新します。

名前	説明
[PLOGI Retries] 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 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	説明
[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 Work 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 [Receive/Transmit Queues] 領域で、次のフィールドを更新します。

名前	説明
[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 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 [Save Changes] をクリックします。

vHBA の作成

アダプタには、2 つの永続 vHBA が用意されています。 NIV モードをイネーブルにすると、最大 16 の追加 vHBA を作成できます。

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Inventory] をクリックします。

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

ステップ 4 [Adapter Cards] 領域で、アダプタ カードを選択します。
サーバの電源をオンにすると、選択したアダプタ カードのリソースが [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 [Adapter Cards] 領域の下のタブ付きメニューで、[vHBAs] タブをクリックします。

ステップ 6 [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、[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 [Clone] をクリックします。

[Add vHBA] ダイアログボックスが表示されます。

ステップ 7 [Add vHBA] ダイアログボックスで、vHBA の名前を [Name] 入力ボックスに入力します。

ステップ 8 [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, （88 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 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Inventory] をクリックします。

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

ステップ 4 [Adapter Cards] 領域で、アダプタ カードを選択します。
サーバの電源をオンにすると、選択したアダプタ カードのリソースが [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 [Adapter Cards] 領域の下のタブ付きメニューで、[vHBAs] タブをクリックします。

ステップ 6 [Host Fibre Channel Interfaces] 領域で、テーブルから vHBA を選択します。

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

ステップ 7 [Delete] をクリックしてから、削除することを確認するために [OK] をクリックします。

vHBA ブート テーブル

vHBA ブート テーブルで、サーバのブート元の LUN を最大 4 個指定できます。

ブート テーブル エントリの作成

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Inventory] をクリックします。

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

ステップ 4 [Adapter Cards] 領域で、アダプタ カードを選択します。
サーバの電源をオンにすると、選択したアダプタ カードのリソースが [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 [Adapter Cards] 領域の下のタブ付きメニューで、[vHBAs] タブをクリックします。

ステップ 6 [Host Fibre Channel Interfaces] 領域で、テーブルから vHBA を選択します。

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

ステップ 8 [Boot Table] ダイアログボックスで、[Add] をクリックして [Add Boot Entry] ダイアログボックスを開きます。

ステップ 9 [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	説明
[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 を 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。 0 ～ 255 の ID を入力します。
[Add Boot Entry] ボタン	指定された場所をブート テーブルに追加します。
[Reset Values] ボタン	フィールドに現在入力されている値をクリアします。

名前	説明
[Cancel] ボタン	ダイアログボックスが開いている間に加えられた変更を保存しないでダイアログボックスを閉じます。

ステップ 10 [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 [Navigation] ペインの [Server] タブをクリックします。
ステップ 2 [Server] タブの [Inventory] をクリックします。
ステップ 3 [Inventory] ペインの [Network Adapters] タブをクリックします。
ステップ 4 [Adapter Cards] 領域で、アダプタ カードを選択します。
サーバの電源をオンにすると、選択したアダプタ カードのリソースが [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 [Adapter Cards] 領域の下のタブ付きメニューで、[vHBAs] タブをクリックします。
ステップ 6 [Host Fibre Channel Interfaces] 領域で、テーブルから vHBA を選択します。
ステップ 7 [Boot Table] をクリックして、選択した vHBA の [Boot Table] ダイアログボックスを開きます。
ステップ 8 [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 [Delete] をクリックしてから、削除することを確認するために [OK] をクリックします。

vHBA の永続的なバインディング

永続的なバインディングにより、ファイバチャネルターゲットのシステムによって割り当てられたマッピングが、リブート後も維持されます。

永続的なバインディングの表示

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Inventory] をクリックします。

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

ステップ 4 [Adapter Cards] 領域で、アダプタ カードを選択します。
サーバの電源をオンにすると、選択したアダプタ カードのリソースが [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 [Adapter Cards] 領域の下のタブ付きメニューで、[vHBAs] タブをクリックします。

ステップ 6 [Host Fibre Channel Interfaces] 領域で、テーブルから vHBA を選択します。

ステップ 7 [Persistent Bindings] をクリックして、選択した vHBA の [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 [Persistent Bindings] ダイアログボックスで、次の情報を確認します。

名前	説明
[Index] カラム	バインディングの固有識別子。
[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 ワールド ワイド ポート名。
[Target LUN] カラム	バインディングが関連付けられるターゲット LUN ID。
[Host LUN] 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 LUN ID。
[Clear Persistent Bindings] ボタン	現在のすべてのバインディングをクリアします。
[Close] ボタン	ダイアログボックスを閉じて変更を保存します。

ステップ 9 [Close] をクリックします。

永続的なバインディングのクリア

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Inventory] をクリックします。

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

ステップ 4 [Adapter Cards] 領域で、アダプタ カードを選択します。
サーバの電源をオンにすると、選択したアダプタ カードのリソースが [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 [Adapter Cards] 領域の下のタブ付きメニューで、[vHBAs] タブをクリックします。

ステップ 6 [Host Fibre Channel Interfaces] 領域で、テーブルから vHBA を選択します。

ステップ 7 [Persistent Bindings] をクリックして、選択した vHBA の [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 [Persistent Bindings] ダイアログボックスで、[Clear Persistent Bindings] をクリックします。

ステップ 9 [Close] をクリックします。

vNIC の管理

vNIC の管理上の注意事項

vNIC を管理するときは、次の注意事項および制約事項を考慮してください。

- Cisco UCS P81E 仮想インターフェイス カードには、2 つのデフォルトの vNIC（eth0 および eth1）があります。 このアダプタ カードでは最大 16 個の vNIC を追加作成できます。

（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である場合は、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、設定を反映するにはホストをリブートする必要があります。

vNIC のプロパティの表示

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Inventory] をクリックします。

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

ステップ 4 [Adapter Cards] 領域で、アダプタ カードを選択します。
サーバの電源をオンにすると、選択したアダプタ カードのリソースが [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 [Adapter Cards] 領域の下のタブ付きメニューで、[vNICs] タブをクリックします。

ステップ 6 [Host Ethernet Interfaces] 領域で、テーブルから vNIC を選択します。

ステップ 7 [Properties] をクリックして、[vNIC Properties] ダイアログボックスを開きます。

ステップ 8 [General] 領域で、次のフィールドの情報を確認します。

名前	説明
[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。
[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。
[Uplink Port] ドロップダウン リスト	この vNIC に関連付けられているアップリンク ポート。 この vNIC のトラフィックはすべてこのアップリンク ポートを通過します。
[MAC Address] フィールド	vNIC に関連付けられている MAC アドレス。 使用可能な MAC アドレスを内部プールから自動的に選択するには、[Auto] を選択します。 アドレスを指定するには、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 MAC アドレスを入力します。
[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 は最低プライオリティを表し、6 は最高プライオリティを表します。 （注） このオプションは、NIV モードでは使用できません。

名前	説明
[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 クラスを使用する場合は、このチェックボックスをオンにします。
[PCI Order] フィールド	この vNIC が使用される順序。 順序を自動的に設定するには、[Any] を選択します。 順序を指定するには、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。
[Default VLAN] フィールド	この vNIC のデフォルト VLAN がない場合は、[NONE] をクリックします。 それ以外の場合は、2 つ目のオプション ボタンをクリックし、フィールドに 1 ～ 4094 の VLAN ID を入力します。 （注） このオプションは、NIV モードでは使用できません。
[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、[TRUNK] を選択します。 それ以外の場合は [ACCESS] を選択します。 （注） このオプションは、NIV モードでは使用できません。
[Rate Limit] フィールド	この vNIC のデータ レートを制限しない場合は、[OFF] を選択します。 それ以外の場合は、2 つ目のオプション ボタンをクリックし、関連付けられたフィールドにレート制限を入力します。 1 ～ 10,000 Mbps の整数を入力します。 （注） このオプションは、NIV モードでは使用できません。
[Enable PXE Boot] チェックボックス	vNIC を使用して PXE ブートを実行できる場合は、このチェックボックスをオンにします。
[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） このオプションでは NIV モードが必要です。
[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、このサーバの接続先スイッチに定義されているポート プロファイルが表示されます。 （注） このオプションでは NIV モードが必要です。

名前	説明
[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） このオプションでは NIV モードが必要です。
[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） このオプションでは NIV モードが必要です。

ステップ 9 [Ethernet Interrupt] 領域で、次のフィールドの情報を確認します。

名前	説明
[Interrupt Count] フィールド	割り当てる割り込みリソースの数。通常、この値は、完了キューリソースの数と同じにします。 1 ～ 514 の整数を入力します。
[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。
[Coalescing Type] ドロップダウン リスト	次のいずれかになります。 • [MIN]：別の割り込みイベントを送信する前に、[Coalescing Time] フィールドに指定された時間だけシステムは待機します。 • [IDLE]：アクティビティなしの期間が少なくとも [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	説明
[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 だけ。 • [INTx]：PCI INTx 割り込み。

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

名前	説明
[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。
[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 [Ethernet Transmit Queue] 領域で、次のフィールドの情報を確認します。

名前	説明
[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。
[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 [Completion Queue] 領域で、次のフィールドの情報を確認します。

名前	説明
[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。
[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 [TCP Offload] 領域で、次のフィールドの情報を確認します。

名前	説明
[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 は大きな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。
[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。
[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。
[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 はすべての大きなパケットを処理します。

ステップ 14 [Receive Side Scaling] 領域で、次のフィールドの情報を確認します。

名前	説明
[Enable TCP Receive Side Scaling] チェックボックス	Receive Side Scaling（RSS）では、マルチプロセッサ システム内の複数の CPU 間で、ネットワーク受信処理を分散させることができます。 オンにすると、ネットワーク受信処理は、可能な場合はいつでもプロセッサ間で分担されます。 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。

名前	説明
[Enable IPv4 RSS] チェックボックス	オンにすると、IPv4 ネットワークで RSS がイネーブルになります。
[Enable TCP-IPv4 RSS] チェックボックス	オンにすると、IPv4 ネットワークで TCP 伝送の RSS がイネーブルになります。
[Enable IPv6 RSS] チェックボックス	オンにすると、IPv6 ネットワークで RSS がイネーブルになります。
[Enable TCP-IPv6 RSS] チェックボックス	オンにすると、IPv6 ネットワークで TCP 伝送の RSS がイネーブルになります。
[Enable IPv6 Extension RSS] チェックボックス	オンにすると、IPv6 拡張の RSS がイネーブルになります。
[Enable TCP-IPv6 Extension RSS] チェックボックス	オンにすると、IPv6 ネットワークで TCP 伝送の 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 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Inventory] をクリックします。

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

ステップ 4 [Adapter Cards] 領域で、アダプタ カードを選択します。
サーバの電源をオンにすると、選択したアダプタ カードのリソースが [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 [Adapter Cards] 領域の下のタブ付きメニューで、[vNICs] タブをクリックします。

ステップ 6 [Host Ethernet Interfaces] 領域で、テーブルから vNIC を選択します。

ステップ 7 [Properties] をクリックして、[vNIC Properties] ダイアログボックスを開きます。

ステップ 8 [General] 領域で、次のフィールドを更新します。

名前	説明
[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。
[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。
[Uplink Port] ドロップダウン リスト	この vNIC に関連付けられているアップリンク ポート。 この vNIC のトラフィックはすべてこのアップリンク ポートを通過します。
[MAC Address] フィールド	vNIC に関連付けられている MAC アドレス。 使用可能な MAC アドレスを内部プールから自動的に選択するには、[Auto] を選択します。 アドレスを指定するには、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 MAC アドレスを入力します。
[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 は最低プライオリティを表し、6 は最高プライオリティを表します。 （注） このオプションは、NIV モードでは使用できません。
[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 クラスを使用する場合は、このチェックボックスをオンにします。
[PCI Order] フィールド	この vNIC が使用される順序。 順序を自動的に設定するには、[Any] を選択します。 順序を指定するには、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。
[Default VLAN] フィールド	この vNIC のデフォルト VLAN がない場合は、[NONE] をクリックします。 それ以外の場合は、2 つ目のオプション ボタンをクリックし、フィールドに 1 ～ 4094 の VLAN ID を入力します。 （注） このオプションは、NIV モードでは使用できません。

名前	説明
[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、[TRUNK] を選択します。 それ以外の場合は [ACCESS] を選択します。 （注） このオプションは、NIV モードでは使用できません。
[Rate Limit] フィールド	この vNIC のデータ レートを制限しない場合は、[OFF] を選択します。 それ以外の場合は、2 つ目のオプション ボタンをクリックし、関連付けられたフィールドにレート制限を入力します。 1 ～ 10,000 Mbps の整数を入力します。 （注） このオプションは、NIV モードでは使用できません。
[Enable PXE Boot] チェックボックス	vNIC を使用して PXE ブートを実行できる場合は、このチェックボックスをオンにします。
[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） このオプションでは NIV モードが必要です。
[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、このサーバの接続先スイッチに定義されているポート プロファイルが表示されます。 （注） このオプションでは NIV モードが必要です。
[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） このオプションでは NIV モードが必要です。
[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） このオプションでは NIV モードが必要です。

ステップ 9 [Ethernet Interrupt] 領域で、次のフィールドを更新します。

名前	説明
[Interrupt Count] フィールド	割り当てる割り込みリソースの数。通常、この値は、完了キュー リソースの数と同じにします。 1 ～ 514 の整数を入力します。
[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。
[Coalescing Type] ドロップダウン リスト	次のいずれかになります。 • [MIN]：別の割り込みイベントを送信する前に、[Coalescing Time] フィールドに指定された時間だけシステムは待機します。 • [IDLE]：アクティビティなしの期間が少なくとも [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。
[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 だけ。 • [INTx]：PCI INTx 割り込み。

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

名前	説明
[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。
[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 [Ethernet Transmit Queue] 領域で、次のフィールドを更新します。

名前	説明
[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。
[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 [Completion Queue] 領域で、次のフィールドを更新します。

名前	説明
[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。
[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 [TCP Offload] 領域で、次のフィールドを更新します。

名前	説明
[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 は大きな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。
[Enable TCP Rx Offload Checksum Validation] チェックボックス	オンにすると、CPU はすべてのパケット チェックサムを検証のためにハードウェアに送信します。 このオプションにより、CPU のオーバーヘッドが削減される可能性があります。 オフにすると、CPU はすべてのパケット チェックサムを検証します。

名前	説明
[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。
[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はすべての大きなパケットを処理します。

ステップ 14 [Receive Side Scaling] 領域で、次のフィールドを更新します。

名前	説明
[Enable TCP Receive Side Scaling] チェックボックス	Receive Side Scaling（RSS）では、マルチプロセッサ システム内の複数のCPU間で、ネットワーク受信処理を分散させることができます。 オンにすると、ネットワーク受信処理は、可能な場合はいつでもプロセッサ間で分担されます。 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。
[Enable IPv4 RSS] チェックボックス	オンにすると、IPv4ネットワークでRSSがイネーブルになります。
[Enable TCP-IPv4 RSS] チェックボックス	オンにすると、IPv4 ネットワークで TCP 伝送の RSS がイネーブルになります。
[Enable IPv6 RSS] チェックボックス	オンにすると、IPv6ネットワークでRSSがイネーブルになります。
[Enable TCP-IPv6 RSS] チェックボックス	オンにすると、IPv6 ネットワークで TCP 伝送の RSS がイネーブルになります。
[Enable IPv6 Extension RSS] チェックボックス	オンにすると、IPv6 拡張の RSS がイネーブルになります。
[Enable TCP-IPv6 Extension RSS] チェックボックス	オンにすると、IPv6 ネットワークで TCP 伝送の RSS がイネーブルになります。

ステップ 15 [Save Changes] をクリックします。

vNIC の作成

アダプタには、2 つの永続 vNIC があります。 最大 16 個の vNIC を追加作成できます。

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Inventory] をクリックします。

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

ステップ 4 [Adapter Cards] 領域で、アダプタ カードを選択します。
サーバの電源をオンにすると、選択したアダプタ カードのリソースが [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 [Adapter Cards] 領域の下のタブ付きメニューで、[vNICs] タブをクリックします。

ステップ 6 [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、[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、その vNIC を選択して [Clone] をクリックします。

[Add vNIC] ダイアログボックスが表示されます。

ステップ 7 [Add vNIC] ダイアログボックスで、vNIC の名前を [Name] 入力ボックスに入力します。

ステップ 8 （任意） [Add vNIC] ダイアログボックスで、vNIC のチャネル番号を [Channel Number] 入力ボックスに入力します。

（注） アダプタで NIV がイネーブルである場合は、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。

ステップ 9 [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, （103 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 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Inventory] をクリックします。

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

ステップ 4 [Adapter Cards] 領域で、アダプタ カードを選択します。
サーバの電源をオンにすると、選択したアダプタ カードのリソースが [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 [Adapter Cards] 領域の下のタブ付きメニューで、[vNICs] タブをクリックします。

ステップ 6 [Host Ethernet Interfaces] 領域で、テーブルから vNIC を選択します。
（注） 2 つのデフォルトの vNIC である [eth0] または [eth1] は削除できません。

ステップ 7 [Delete] をクリックしてから、削除することを確認するために [OK] をクリックします。

VM FEX の管理

仮想マシン ファブリック エクステンダ

Cisco 仮想マシン ファブリック エクステンダ（VM FEX）によって、（先行標準）IEEE 802.1Qbh ポート エクステンダ アーキテクチャが仮想マシンに拡張されます。 このアーキテクチャでは、各 VM インターフェイスに、仮想 Peripheral Component Interconnect Express（PCIe）デバイスとスイッチ上の仮想ポートが提供されます。

仮想 FEX 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。
- Cisco UCS P81E 仮想インターフェイス カードをシャーシに取り付けて、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 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Inventory] をクリックします。

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

ステップ 4 [Adapter Cards] 領域で、アダプタ カードを選択します。
サーバの電源をオンにすると、選択したアダプタ カードのリソースが [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 [Adapter Cards] 領域の下のタブ付きメニューで、[VM FEXs] タブをクリックします。

ステップ 6 [Virtual FEXs] 領域で、次の情報を確認します。

名前	説明
[Properties] ボタン	選択した VM FEX のプロパティを表示できるダイアログボックスを開きます。
[Name] カラム	VM FEX の名前。
[MTU] カラム	この VM FEX で受け入れられる最大伝送単位、つまりパケット サイズ。
[CoS] カラム	イネーブルにすると、VM FEX はホスト オペレーティング システムが提供するサービス クラスを使用します。
[VLAN] カラム	VM FEX に関連付けられている VLAN。
[VLAN Mode] カラム	関連付けられた VLAN のモード。
[Uplink Failover] カラム	アダプタで NIV モードがイネーブルの場合、このカラムには、プライマリ インターフェイスで障害が発生したときにこの VM FEX 上のトラフィックがセカンダリ インターフェイスにフェールオーバーするかどうかが表示されます。

ステップ 7 [Virtual FEXs] 領域で、VM FEX をテーブルから選択します。

ステップ 8 [Properties] をクリックして、選択した VM FEX の [VM FEX Properties] ダイアログボックスを開きます。

ステップ 9 [General Properties] 領域で、次のフィールドの情報を確認します。

名前	説明
[Name] フィールド	VM FEX の名前。

名前	説明
[MTU] フィールド	この VM FEX で受け入れられる最大伝送単位、つまりパケット サイズ。
[Trust Host CoS] フィールド	イネーブルにすると、VM FEX はホスト オペレーティング システムが提供するサービス クラスを使用します。
[PCI Order] フィールド	この VM FEX が使用される順序（ある場合）。
[Default VLAN] フィールド	VM FEX に関連付けられている VLAN。
[Rate Limit] フィールド	この VM FEX に関連付けられているデータ レート制限（ある場合）。
[PXE Boot] フィールド	この VM FEX に対して PXE ブートをイネーブルにするかディセーブルにするか。

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

名前	説明
[Interrupt Count] フィールド	この VM FEX に割り当てる割り込みリソースの数。
[Coalescing Time] フィールド	割り込み間の CIMC 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。
[Coalescing Type] フィールド	次のいずれかになります。 • [MIN]：別の割り込みイベントを送信する前に、[Coalescing Time] フィールドに指定された時間だけシステムは待機します。 • [IDLE]：アクティビティなしの期間が少なくとも [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。
[Interrupt Mode] フィールド	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）。 • [MSI]：MSI だけ。 • [INTx]：PCI INTx 割り込み。

ステップ 11 [Ethernet Receive Queue] 領域で、次のフィールドの情報を確認します。

名前	説明
[Receive Queue Count] フィールド	この VM FEX に割り当てる受信キュー リソースの数。
[Receive Queue Ring Size] フィールド	各受信キュー内の記述子の数。

ステップ 12 [Ethernet Transmit Queue] 領域で、次のフィールドの情報を確認します。

名前	説明
[Transmit Queue Count] フィールド	この VM FEX に割り当てる送信キュー リソースの数。
[Transmit Queue Ring Size] フィールド	各送信キュー内の記述子の数。

ステップ 13 [Completion Queue] 領域で、次のフィールドの情報を確認します。

名前	説明
[Completion Queue Count] フィールド	この VM FEX に割り当てる完了キュー リソースの数。
[Completion Queue Ring Size] フィールド	各完了キュー内の記述子の数。

ステップ 14 [TCP Offload] 領域で、次のフィールドの情報を確認します。

名前	説明
[Enable TCP Segmentation Offload] フィールド	イネーブルにすると、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。 ディセーブルにすると、CPU は大きな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。
[Enable TCP Rx Offload Checksum Validation] フィールド	イネーブルにすると、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。 ディセーブルにすると、CPU はすべてのパケット チェックサムを検証します。

名前	説明
[Enable TCP Tx Offload Checksum Generation] フィールド	イネーブルにすると、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。ディセーブルにすると、CPUはすべてのパケットチェックサムを計算します。
[Enable Large Receive] フィールド	イネーブルにすると、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。 ディセーブルにすると、CPUはすべての大きなパケットを処理します。

ステップ 15 [Receive Side Scaling] 領域で、次のフィールドの情報を確認します。

名前	説明
[Enable TCP Receive Side Scaling] フィールド	Receive Side Scaling（RSS）では、マルチプロセッサ システム内の複数のCPU間で、ネットワーク受信処理を分散させることができます。 イネーブルにすると、ネットワーク受信処理は、可能な場合はいつでもプロセッサ間で分担されます。 ディセーブルにすると、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。
[Enable IPv4 RSS] フィールド	イネーブルにすると、IPv4ネットワークでRSSがイネーブルになります。
[Enable TCP-IPv4 RSS] フィールド	イネーブルにすると、IPv4 ネットワークでの TCP 伝送で RSS がイネーブルになります。
[Enable IPv6 RSS] フィールド	イネーブルにすると、IPv6ネットワークでRSSがイネーブルになります。
[Enable TCP-IPv6 RSS] フィールド	イネーブルにすると、IPv6 ネットワークでの TCP 伝送で RSS がイネーブルになります。
[Enable IPv6 Extension RSS] フィールド	イネーブルにすると、IPv6 拡張の RSS がイネーブルになります。
[Enable TCP-IPv6 Extension RSS] フィールド	イネーブルにすると、IPv6 ネットワークでの TCP 伝送で RSS がイネーブルになります。

アダプタ構成のバックアップと復元

アダプタ構成のエクスポート

アダプタ構成を XML ファイルとして TFTP サーバにエクスポートできます。

はじめる前に

TFTP サーバの IP アドレスを取得します。

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Inventory] をクリックします。

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

ステップ 4 [Adapter Cards] 領域で、アダプタ カードを選択します。
サーバの電源をオンにすると、選択したアダプタ カードのリソースが [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 [Adapter Cards] 領域の下のタブ付きメニューで、[General] タブをクリックします。

ステップ 6 [General] タブの [Actions] 領域で、[Export Configuration] をクリックします。
[Export Adapter Configuration] ダイアログボックスが開きます。

ステップ 7 [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	説明
[TFTP Server IP Address] フィールド	アダプタ構成ファイルのエクスポート先の TFTP サーバの IP アドレス。
[Path and Filename] フィールド	ファイルを TFTP サーバにエクスポートするときに CIMC によって使用されるパスおよびファイル名。

ステップ 8 [Export Configuration] をクリックします。

アダプタ構成のインポート

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Inventory] をクリックします。

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

ステップ 4 [Adapter Cards] 領域で、アダプタ カードを選択します。
サーバの電源をオンにすると、選択したアダプタ カードのリソースが [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 [Adapter Cards] 領域の下のタブ付きメニューで、[General] タブをクリックします。

ステップ 6 [General] タブの [Actions] 領域で、[Import Configuration] をクリックします。
[Import Adapter Configuration] ダイアログボックスが開きます。

ステップ 7 [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	説明
[TFTP Server IP Address] フィールド	アダプタ構成ファイルが存在する TFTP サーバの IP アドレス。
[Path and Filename] フィールド	TFTP サーバ上の構成ファイルのパスおよびファイル名。

ステップ 8 [Import Configuration] をクリックします。
アダプタによって、指定の IP アドレスにある TFTP サーバ上の指定のパスから、構成ファイルがダウンロードされます。 構成はサーバの次のリブート時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、インポートした構成を適用します。

アダプタのデフォルトの復元

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Inventory] をクリックします。

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

ステップ 4 [Adapter Cards] 領域で、アダプタ カードを選択します。
サーバの電源をオンにすると、選択したアダプタ カードのリソースが [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 [Adapter Cards] 領域の下のタブ付きメニューで、[General] タブをクリックします。

ステップ 6 [General] タブの [Actions] 領域で、[Reset To Defaults] をクリックし、[OK] をクリックして確認します。

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、CIMC GUI または CLI インターフェイスから、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、CIMC GUI または CLI 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 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Inventory] をクリックします。

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

ステップ 4 [Adapter Cards] 領域で、アダプタ カードを選択します。
サーバの電源をオンにすると、選択したアダプタ カードのリソースが [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 [Adapter Cards] 領域の下のタブ付きメニューで、[General] タブをクリックします。

ステップ 6 [General] タブの [Actions] 領域で、[Install Firmware] をクリックして [Install Adapter Firmware] ダイアログボックスを開きます。

ステップ 7 [Install Adapter Firmware] ダイアログボックスで、[Install from local file] を選択し、[Next] をクリックします。

ステップ 8 [Browse...] をクリックして、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 [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アクティブにするには、「アダプタ ファームウェアのアクティブ化」を参照してください。

TFTP 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 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Inventory] をクリックします。

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

ステップ 4 [Adapter Cards] 領域で、アダプタ カードを選択します。
サーバの電源をオンにすると、選択したアダプタ カードのリソースが [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 [Adapter Cards] 領域の下のタブ付きメニューで、[General] タブをクリックします。

ステップ 6 [General] タブの [Actions] 領域で、[Install Firmware] をクリックして [Install Adapter Firmware] ダイアログボックスを開きます。

ステップ 7 [Install Adapter Firmware] ダイアログボックスで、[Install from TFTP server] を選択し、[Next] をクリックします。

ステップ 8 [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	説明
[TFTP Server IP Address] フィールド	アダプタ構成ファイルが存在する TFTP サーバの IP アドレス。
[Path and Filename] フィールド	TFTP サーバ上の構成ファイルのパスおよびファイル名。
[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。
[Install Firmware] ボタン	このボタンをクリックして、選択したファームウェア パッケージをアダプタのバックアップ メモリ スロットにインストールします。
[Close] ボタン	サーバに保存されているファームウェア バージョンを変更しないでウィザードを閉じるには、このボタンをクリックします。

ステップ 9 [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アクティブにするには、「アダプタ ファームウェアのアクティブ化」を参照してください。

アダプタ ファームウェアのアクティブ化

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [Inventory] をクリックします。

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

ステップ 4 [Adapter Cards] 領域で、アダプタ カードを選択します。
サーバの電源をオンにすると、選択したアダプタ カードのリソースが [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 [Adapter Cards] 領域の下のタブ付きメニューで、[General] タブをクリックします。

ステップ 6 [General] タブの [Actions] 領域で、[Activate Firmware] をクリックして [Activate Adapter Firmware] ダイアログボックスを開きます。

ステップ 7 [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されるイメージを選択します。

ステップ 8 [Activate Adapter Firmware] をクリックします。

第 10 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，121 ページ
- SSH の設定，122 ページ
- XML API の設定，123 ページ
- IPMI の設定，124 ページ
- SNMP の設定，126 ページ

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 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Communications Services] をクリックします。

ステップ 3 [Communications Services] ペインの [Communication Services] タブをクリックします。

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

名前	説明
[HTTP/S Enabled] チェックボックス	HTTP および HTTPS が CIMC でイネーブルかディセーブルか。

名前	説明
[Redirect HTTP to HTTPS Enabled] チェックボックス	イネーブルにすると、HTTP 経由のすべての通信試行は、同等の HTTPS アドレスにリダイレクトされます。 HTTP をイネーブルにする場合は、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 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 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。
[Session Timeout] フィールド	HTTP 要求の間、CIMC がタイム アウトしてセッションを終了するまで待機する秒数。 60 ～ 10,800 の範囲の整数を入力します。 デフォルトは 1,800 秒です。
[Max Sessions] フィールド	CIMC 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。
[Active Sessions] フィールド	CIMC 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 [Save Changes] をクリックします。

SSH の設定

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 [Navigation] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブの [Communications Services] をクリックします。
ステップ 3 [Communications Services] ペインの [Communication Services] タブをクリックします。
ステップ 4 [SSH Properties] 領域で、次のプロパティを更新します。

名前	説明
[SSH Enabled] チェックボックス	SSH が CIMC でイネーブルかディセーブルか。
[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。 デフォルトは 22 です。
[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 の範囲の整数を入力します。 デフォルトは 1,800 秒です。
[Max Sessions] フィールド	CIMC 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。
[Active Sessions] フィールド	CIMC で現在実行されている SSH セッションの数。

ステップ 5 [Save Changes] をクリックします。

XML API の設定

CIMC の XML API

Cisco CIMC XML アプリケーション プログラミング インターフェイス（API）は、C シリーズ ラックマウント サーバの CIMC に対するプログラミング インターフェイスです。 この API は、HTTP または HTTPS を使用して 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 CIMC 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 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Communications Services] をクリックします。

ステップ 3 [Communications Services] ペインの [Communication Services] タブをクリックします。

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

名前	説明
[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、許可されていないか。
[Max Sessions] フィールド	CIMC 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。
[Active Sessions] フィールド	CIMC で現在実行されている API セッションの数。

ステップ 5 [Save Changes] をクリックします。

IPMI の設定

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、CIMC 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 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Communications Services] をクリックします。

ステップ 3 [Communications Services] ペインの [Communication Services] タブをクリックします。

ステップ 4 [IPMI over LAN Properties] 領域で、次のプロパティを更新します。

名前	説明
[Enabled] 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、許可されていないか。
[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ることができる最も高い特権レベル。 次のいずれかになります。 • [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すると、「Administrator」、「Operator」、または「User」ユーザ ロールを持つ IPMI ユーザは、その他の IPMI 特権に関係なく、読み取り専用 IPMI セッションのみを作成できます。 • [user]：IPMI ユーザは、一部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すると、「Administrator」または「Operator」ユーザ ロールを持つ IPMI ユーザは、このサーバでユーザおよび読み取り専用セッションを作成できます。 • [admin]：IPMI ユーザは、実行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すると、「Administrator」ユーザ ロールを持つ IPMI ユーザは、このサーバで管理、ユーザ、および読み取り専用セッションを作成できます。
[Encryption Key] フィールド	IPMI 通信に使用する IPMI 暗号キー。

ステップ 5 [Save Changes] をクリックします。

SNMP の設定

SNMP

Cisco UCS C シリーズ ラックマウント サーバでは、サーバの設定とステータスの表示および SNMP トラップによる障害およびアラート情報の送信のために、簡易ネットワーク管理プロトコル（SNMP）がサポートされています。CIMC 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/en/US/docs/unified_computing/ucs/sw/mib/reference/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 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Communications Services] をクリックします。

ステップ 3 [Communications Services] ペインの [SNMP] タブをクリックします。

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

名前	説明
[Enabled] チェックボックス	このサーバから指定されたホストまで SNMP トラップを送信するかどうか。
[SNMP Port] フィールド	サーバで SNMP ホストと通信するために使用するポート。 この値は変更できません。
[Access Community String] フィールド	CIMC が SNMP ホストに送信するトラップ メッセージに含まれるデフォルトの SNMP v1 または v2c コミュニティ名あるいは SNMP v3 ユーザ名。 最大 18 文字の文字列を入力します。
[System Contact] フィールド	SNMP 実装のシステム連絡先担当者。 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。

名前	説明
[System Location] フィールド	SNMP エージェント（サーバ）が実行されているホストの場所。 最大 64 文字の文字列を入力します。

ステップ 5 [Save Changes] をクリックします。

次の作業

SNMP トラップ設定の指定, （127 ページ）の説明に従って、SNMP トラップ設定を指定します。

SNMP トラップ設定の指定

はじめる前に

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

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Communications Services] をクリックします。

ステップ 3 [Communications Services] ペインの [SNMP] タブをクリックします。

ステップ 4 [Common Trap Destination Settings] 領域で、次のフィールドに入力します。

名前	説明
[Trap Community String] フィールド	トラップ情報の送信先となる SNMP コミュニティ グループの名前。
[SNMP Version] ドロップダウン リスト	トラップに使用される SNMP バージョンとモデル。 次のいずれかになります。 • V1 • V2 • V3
[Type] フィールド	バージョンとして [V2] を選択した場合、このタイプのトラップが送信されます。 次のいずれかになります。 • Trap • Inform

ステップ 5 [Trap Destinations] 領域で、次のフィールドに入力します。

名前	説明
[ID] カラム	トラップの宛先 ID。 この値は変更できません。
[Enabled] カラム	使用する SNMP トラップの宛先ごとに、このカラムの対応するチェックボックスをオンにします。
[Trap Destination IP Address] カラム	SNMP トラップ情報の送信先の IP アドレス。

ヒント トラップの設定を変更したり、テスト トラップ メッセージを送信したりする場合、管理者はテーブルのトラップ行をクリックできます。

ステップ 6 [Save Changes] をクリックします。

SNMP テスト 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 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Event Management] をクリックします。

ステップ 3 [Event Management] ペインの [Trap Settings] タブをクリックします。

ステップ 4 [Trap Destinations] 領域で、目的の SNMP トラップの宛先の行をクリックします。
[Traps Details] ダイアログボックスが開きます。

ステップ 5 [Send SNMP trap] をクリックします。
SNMPv1 テスト トラップ メッセージがトラップの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、トラップが設定され、イネーブルである必要があります。

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 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Communications Services] をクリックします。

ステップ 3 [Communications Services] ペインの [SNMP] タブをクリックします。

ステップ 4 [SNMPV3 Users] 領域で、次のプロパティを更新します。

名前	説明
[Add] ボタン	テーブルで使用可能な行をクリックし、このボタンをクリックして新しい SNMP ユーザを追加します。
[Modify] ボタン	テーブル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。
[Delete] ボタン	テーブル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	システムによって SNMP ユーザに割り当てられた ID。
[Name] カラム	SNMP ユーザ名。
[Auth Type] カラム	ユーザ認証タイプ。
[Privacy Type] カラム	ユーザ プライバシー タイプ。

ステップ 5 [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 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Communications Services] をクリックします。

ステップ 3 [Communications Services] ペインの [SNMP] タブをクリックします。

ステップ 4 [SNMPV3 Users] 領域で、次のアクションのいずれかを実行します。

- 既存のユーザをテーブルから選択し、[Modify] をクリックします。
- [Add] をクリックし、新しいユーザを作成します。

（注） ボタンがディセーブルの場合は、SNMP をイネーブルにして [Save Changes] をクリックします。

ステップ 5 [SNMPV3 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	説明
[ID] フィールド	ユーザの固有識別情報。 このフィールドは変更できません。
[Name] フィールド	SNMP ユーザ名。
[Security Level] ドロップダウンリスト	このユーザのセキュリティ レベル。 次のいずれかになります。 • [no auth, no priv]：ユーザには許可パスワードまたはプライバシー パスワードが必要ありません。 • [auth, no priv]：ユーザには許可パスワードが必要ですが、プライバシーパスワードは必要ありません。 このオプションを選択すると、CIMC で後述の許可フィールドがイネーブルになります。 • [auth, priv]：ユーザには許可パスワードとプライバシー パスワードの両方が必要です。 このオプションを選択すると、CIMC で許可フィールドとプライバシー フィールドがイネーブルになります。
[Auth Type] フィールド	許可タイプ。 次のいずれかになります。 • MD5 • SHA
[Auth Password] フィールド	この SNMP ユーザの許可パスワード。

名前	説明
[Confirm Auth Password] フィールド	確認のための許可パスワードの再入力。
[Privacy Type] フィールド	プライバシー タイプ。 次のいずれかになります。 • DES • AES
[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。
[Confirm Privacy Password] フィールド	確認のための許可パスワードの再入力。

ステップ 6 [Save Changes] をクリックします。

第 11 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，133 ページ
- 証明書署名要求の生成，134 ページ
- 自己署名証明書の作成，135 ページ
- サーバ証明書のアップロード，137 ページ

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 CIMC 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 Certificate Authority（CA; 認証局）、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。

手順

ステップ 1 CIMC 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 CIMC にアップロードします。

（注） アップロードされた証明書は、CIMC によって生成された CSR から作成される必要があります。 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

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。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Certificate Management] をクリックします。

ステップ 3 [Actions] 領域で、[Generate New Certificate Signing Request] リンクをクリックします。
[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 [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	説明
[Common Name] フィールド	CIMC の完全修飾ホスト名
[Organization Name] フィールド	証明書を要求している組織。
[Organization Unit] フィールド	組織ユニット
[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。
[State Name] フィールド	証明書を要求している会社の本社が存在する州または行政区分。
[Country Code] ドロップダウンリスト	会社が存在する国。
[Email] フィールド	会社の電子メールの連絡先。

ステップ 5 [Generate CSR] をクリックします。
[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) [Open With] をクリックして csr.txt を表示します。

b) [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。

自己署名証明書の作成

パブリック Certificate Authority（CA; 認証局）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、CIMC CLI 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。

手順

	コマンドまたはアクション	目的
ステップ 1	**openssl genrsa -out** *CA_keyfilename keysize* 例： `# openssl genrsa -out ca.key 1024`	このコマンドは、CA で使用される RSA 秘密キーを生成します。 （注） ユーザ入力なしで CA がキーにアクセスできるように、このコマンドに -des3 オプションは使用しないでください。 指定されたファイル名には、指定されたサイズの RSA キーが含まれています。
ステップ 2	**openssl req -new -x509 -days** *numdays* **-key** *CA_keyfilename* **-out** *CA_certfilename* 例： `# openssl req -new -x509 -days 365 -key ca.key -out ca.crt`	このコマンドは、指定されたキーを使用して、CA の自己署名証明書を新規に作成します。 証明書は指定された期間有効になります。 このコマンドは、ユーザに証明書の追加情報を求めるプロンプトを表示します。 証明書サーバは、アクティブな CA です。
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 コンフィギュレーション 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 コンフィギュレーション ファイル openssl.conf には、"nsCertType = server" という文が含まれています。

	コマンドまたはアクション	目的
ステップ 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。

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 1024
Generating RSA private key, 1024 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 CIMC にアップロードします。

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。

（注） [CIMC Certificate Management] メニューを使用して最初に CSR を生成してから、その CSR を使用してアップロードする証明書を取得する必要があります。 この方法で取得されていない証明書はアップロードしないでください。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Certificate Management] をクリックします。

ステップ 3 [Actions] 領域で、[Upload Server Certificate] をクリックします。
[Upload Certificate] ダイアログボックスが表示されます。

ステップ 4 [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	説明
[File] フィールド	アップロードする証明書ファイル。
[Browse] ボタン	適切な証明書ファイルに移動できるダイアログボックスが表示されます。

ステップ 5 [Upload Certificate] をクリックします。

第 12 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，139 ページ
- プラットフォーム イベント アラートのイネーブル化，140 ページ
- プラットフォーム イベント アラートのディセーブル化，140 ページ
- プラットフォーム イベント フィルタの設定，140 ページ
- SNMP トラップ設定の指定，142 ページ
- SNMP テスト トラップ メッセージの送信，143 ページ
- プラットフォーム イベント トラップの解釈，143 ページ

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、ハードウェア関連の重要なイベントが発生したときに、アクションをトリガーしたりアラートを生成したりできます。 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。 また、プラットフォームイベントが発生したときにアラートを生成して送信することもできます。 アラートは SNMP トラップとして送信されるので、アラートを送信するには、先に SNMP トラップの宛先を設定する必要があります。

プラットフォームイベントアラートの生成はグローバルにイネーブルまたはディセーブルにできます。 ディセーブルにすると、PEF がアラートを送信するように設定されていても、アラートは送信されません。

プラットフォーム イベント アラートのイネーブル化

はじめる前に

プラットフォーム イベント アラート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 [Navigation] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブの [Event Management] をクリックします。
ステップ 3 [Event Management] ペインの [Platform Event Filters] タブをクリックします。
ステップ 4 [Platform Event Alerts] 領域で、[Enable Platform Event Alerts] チェックボックスをオンにします。
ステップ 5 [Save Changes] をクリックします。

プラットフォーム イベント アラートのディセーブル化

はじめる前に

プラットフォーム イベント アラート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 [Navigation] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブの [Event Management] をクリックします。
ステップ 3 [Event Management] ペインの [Platform Event Filters] タブをクリックします。
ステップ 4 [Platform Event Alerts] 領域で、[Enable Platform Event Alerts] チェックボックスをオフにします。
ステップ 5 [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。

プラットフォーム イベント フィルタの設定

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Event Management] をクリックします。

ステップ 3 [Event Management] ペインの [Platform Event Filters] タブをクリックします。

ステップ 4 [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	説明
[ID] カラム	一意のフィルタ ID。
[Event] カラム	イベント フィルタの名前。
[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。 • [None]：アクションが実行されません。 • [Reboot]：サーバがリブートされます。 • [Power Cycle]：サーバの電源が再投入されます。 • [Power Off]：サーバの電源がオフになります。
[Send Alert] カラム	アラートを送信するフィルタごとに、このカラムの対応するチェックボックスを選択します。 （注） アラートを送信するには、フィルタ トラップの設定を正しく指定し、[Enable Platform Event Filters] チェックボックスもオンにする必要があります。

ステップ 5 [Save Changes] をクリックします。

次の作業

PEF を設定してアラートを送信する場合は、次のタスクを完了させます。

- プラットフォーム イベント アラートのイネーブル化, （140 ページ）
- SNMP トラップ設定の指定, （127 ページ）

SNMP トラップ設定の指定

はじめる前に

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

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Communications Services] をクリックします。

ステップ 3 [Communications Services] ペインの [SNMP] タブをクリックします。

ステップ 4 [Common Trap Destination Settings] 領域で、次のフィールドに入力します。

名前	説明
[Trap Community String] フィールド	トラップ情報の送信先となる SNMP コミュニティ グループの名前。
[SNMP Version] ドロップダウン リスト	トラップに使用される SNMP バージョンとモデル。 次のいずれかになります。 • V1 • V2 • V3
[Type] フィールド	バージョンとして [V2] を選択した場合、このタイプのトラップが送信されます。 次のいずれかになります。 • Trap • Inform

ステップ 5 [Trap Destinations] 領域で、次のフィールドに入力します。

名前	説明
[ID] カラム	トラップの宛先 ID。 この値は変更できません。
[Enabled] カラム	使用する SNMP トラップの宛先ごとに、このカラムの対応するチェックボックスをオンにします。
[Trap Destination IP Address] カラム	SNMP トラップ情報の送信先の IP アドレス。

ヒント　トラップの設定を変更したり、テスト トラップ メッセージを送信したりする場合、管理者はテーブルのトラップ行をクリックできます。

ステップ 6　[Save Changes] をクリックします。

SNMP テスト 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　[Navigation] ペインの [Admin] タブをクリックします。

ステップ 2　[Admin] タブの [Event Management] をクリックします。

ステップ 3　[Event Management] ペインの [Trap Settings] タブをクリックします。

ステップ 4　[Trap Destinations] 領域で、目的の SNMP トラップの宛先の行をクリックします。
[Traps Details] ダイアログボックスが開きます。

ステップ 5　[Send SNMP trap] をクリックします。
SNMPv1 テスト トラップ メッセージがトラップの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、トラップが設定され、イネーブルである必要があります。

プラットフォーム イベント トラップの解釈

SNMP トラップとして送信される CIMC プラットフォーム イベント アラートには、エンタープライズ オブジェクト ID（OID）が `1.3.6.1.4.1.3183.1.1.0.event` という形式で含まれています。OID の最初の 10 個のフィールドが表している情報は、
`iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).wired_for_management(3183).PET(1).version(1).version(0)`
であり、IPMI プラットフォーム イベント トラップ（PET）バージョン 1.0 メッセージを示しています。 最後のフィールドはイベント番号であり、通知される特定の条件またはアラートを示しています。

プラットフォーム イベント トラップの説明

次の表は、プラットフォーム イベント トラップ メッセージで通知されるイベントの説明です。トラップ OID のイベント番号に基づいています。

イベント番号 [注記 1]		プラットフォーム イベントの説明
0	0h	テスト トラップ
65799	010107h	温度警告
65801	010109h	温度緊急
131330	020102h	電圧不足、緊急
131337	020109h	電圧緊急
196871	030107h	電流警告
262402	040102h	ファン緊急
459776	070400h	プロセッサ関連（IOH-Thermalert/Caterr センサー）：予測障害非アサート
459777	070401h	プロセッサ関連（IOH-Thermalert/Caterr センサー）：予測障害アサート
460032	070500h	プロセッサ電力警告：制限未超過
460033	070501h	プロセッサ電力警告：制限超過
524533	0800F5h	電源緊急
524551	080107h	電源警告
525313	080401h	ディスクリート電源警告
527105	080B01h	電源冗長性損失
527106	080B02h	電源冗長性復元
552704	086F00h	電源挿入
552705	086F01h	電源モジュール障害
552707	086F03h	電源装置 AC 損失
786433	0C0001h	修正可能な ECC メモリ エラー、リリース 1.3(1) 以降のリリース、すべての読み取りタイプを受け入れるように設定されたフィルタ [注記 4]
786439	0C0007h	DDR3_INFO センサー LED：RED ビット アサート（DIMM での ECC エラーの可能性が高い）、汎用センサー [注記 2、3]
786689	0C0101h	修正可能な ECC メモリ エラー、リリース 1.3(1) 以降のリリース
818945	0C7F01h	修正可能な ECC メモリ エラー、リリース 1.2(x) 以前のリリース

イベント番号 [注記 1]		プラットフォーム イベントの説明
818951	0C7F07h	DDR3_INFO センサー LED：RED ビット アサート（DIMM での ECC エラーの可能性が高い）、1.2(x) 以前のリリース [注記 3]
851968	0D0000h	HDD センサーで障害が示されない、汎用センサー [注記 2]
851972	0D0004h	HDD センサーで障害が示される、汎用センサー [注記 2]
854016	0D0800h	HDD が存在しない、汎用センサー [注記 2]
854017	0D0801h	HDD が存在する、汎用センサー [注記 2]
880384	0D6F00h	HDD が存在する、障害なし
880385	0D6F01h	HDD 障害
880512	0D6F80h	HDD が存在しない
880513	0D6F81h	HDD が非アサートだが、障害状態ではない
884480	0D7F00h	ドライブ スロット LED オフ
884481	0D7F01h	ドライブ スロット LED オン
884482	0D7F02h	ドライブ スロット LED 高速で点滅
884483	0D7F03h	ドライブ スロット LED 低速で点滅
884484	0D7F04h	ドライブ スロット LED 緑
884485	0D7F05h	ドライブ スロット LED オレンジ
884486	0D7F01h	ドライブ スロット LED 青
884487	0D7F01h	ドライブ スロット LED 読み取り
884488	0D7F08h	ドライブ スロット オンライン
884489	0D7F09h	ドライブ スロット低下
注記 1：イベント番号の書式の基本情報については、次の URL にある『*IPMI Platform Event Trap Format Specification v1.0*』を参照してください。ftp://download.intel.com/design/servers/ipmi/pet100.pdf		
注記 2：一部のプラットフォームおよびリリースでは汎用センサー実装が使用され、一部のプラットフォームおよびリリースではシスコ独自のセンサー実装が使用されます。		
注記 3：リリース 1.3(1) 以降のリリースでは、ECC センサーによって LED はアクティブ化されなくなりました。		
注記 4：すべての読み取りタイプを受け入れるようにイベント フィルタが設定された場合は、16 進のイベント番号のビット 15:8 は 0 にマスクされます。 たとえば、イベント番号 786689（0C0101h）は 786433（0C0001h）になります。		

第 13 章

CIMC 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，147 ページ
- シスコからの CIMC ファームウェアの取得，148 ページ
- TFTP サーバからの CIMC ファームウェアのインストール，149 ページ
- ブラウザ経由の CIMC ファームウェアのインストール，150 ページ
- インストールされている CIMC ファームウェアのアクティブ化，151 ページ
- TFTP サーバからの BIOS ファームウェアのインストール，152 ページ
- ブラウザ経由の BIOS ファームウェアのインストール，152 ページ

ファームウェアの概要

C シリーズサーバは、cisco.com からダウンロードされたファームウェアを使用します。 このファームウェアでは、C シリーズ サーバのファームウェアをアップグレードすることがシスコによって認可されています。

ダウンロードするファームウェアは、.zip ファイルにパッケージ化されています。 シスコからファームウェアの .zip ファイルをダウンロードした後、これを使用してサーバのファームウェアを更新することができます。 また、シスコでは各イメージのリリース ノートも提供しており、イメージを取得したのと同じ Web サイトから入手できます。

警告 .zip ファイルを使用してサーバの再イメージ化を行わないでください。

再イメージ化には .bin ファイルを使用します。 この .zip ファイルから適切な .bin アップグレードファイルを展開する必要があります。 この .bin ファイルは、TFTP サーバまたはローカル マシンに展開できます。 または で参照したように、再イメージ化は TFTP サーバまたはローカル マシンのブラウザを使用して行うことができます。

（注） ファームウェアを更新するときは、古いバージョンのファームウェアを新しいバージョンのファームウェアにアップグレードすることも、新しいバージョンのファームウェアを古いバージョンのファームウェアにダウングレードすることもできます。

CIMC は、サーバの実行中にアップタイムに影響を与えることなくファームウェアをコンポーネントにインストールできるように、ファームウェアの更新プロセスを段階的に分けています。 アクティブにするまでサーバを再起動する必要がないため、夜間やその他のメンテナンス期間にこのタスクを実行することができます。 ファームウェアの更新は、次の段階で行われます。

インストール

この段階では、CIMC は選択されたファームウェア バージョンをサーバに転送します。 インストールプロセスでは、サーバ上の非アクティブ スロット内のファームウェアが常に上書きされます。 ファームウェアは次のいずれかの方法でインストールできます。

- ブラウザ クライアント経由：コンピュータ上でファームウェア イメージを参照し、サーバにインストールできます。
- TFTP サーバから：TFTP サーバにあるファームウェア イメージをインストールできます。

アクティブ化

この段階では、CIMC 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し、サーバを再起動します。 サーバを再起動すると、非アクティブ スロットはアクティブ スロットになり、アクティブ スロットは非アクティブ スロットになります。 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となります。

シスコからの CIMC ファームウェアの取得

手順

ステップ 1 cisco.com に移動します。

ステップ 2 最上部のツールバーで、[Support] をクリックし、ドロップダウン メニューから [Software Download] を選択します。

ステップ 3 左下隅にある [Unified Computing] リンクをクリックしてからログインします。

ステップ 4 [Cisco C-Series Rack-Mount Servers] ノードを展開し、Cisco C シリーズ ラックマウント サーバの各モデルへのリンクを表示します。

ステップ 5 サーバ モデルの適切なリンクをクリックします。

ステップ 6 [Unified Computing System (UCS) Integrated Management Controller Firmware] リンクをクリックしてから、適切なリリース バージョンのリンクをクリックします。

ステップ 7 [Download Now] をクリックします。

[Download Cart] ダイアログボックスが表示されます。

ステップ 8 [Download Cart] ダイアログボックスの情報を確認してから、[Proceed with Download] をクリックします。
[Software Download Rules] ページが表示されます。

ステップ 9 ダウンロード ルールを確認してから、[Agree] をクリックします。
ダウンロード内容を示すダイアログボックスが表示されます。 [Select Location] ダイアログボックスも表示されます。 このダイアログボックスにフォーカスが置かれます。

ステップ 10 [Select Location] ダイアログボックスで場所を選択し、[Open] をクリックします。
ダウンロードが開始します。

ステップ 11 ダウンロードが終了したら、[Close] をクリックします。
ダウンロードしたファイルは、.zip ファイルです。

警告 .zip ファイルを使用してサーバの再イメージ化を行わないでください。

再イメージ化には .bin ファイルを使用します。 この .zip ファイルから適切な .bin アップグレード ファイルを展開する必要があります。 この .bin ファイルは、TFTP サーバまたはローカル マシンに展開できます。 または で参照したように、再イメージ化は TFTP サーバまたはローカル マシンのブラウザを使用して行うことができます。

展開した適切な .bin ファイルの名前は、再イメージ化しているモデル サーバによって異なります。 1.0.2 ファームウェアの更新ファイルの例を次のとおりです。

- C200 および C210：upd-pkg-c200-m1-cimc.full.1.0.2.bin
- C250：upd-pkg-c250-m1-cimc.full.1.0.2.bin

次の作業

CIMC ファームウェアをサーバにインストールします。

TFTP サーバからの CIMC ファームウェアのインストール

はじめる前に

- CIMC ファームウェア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。
- シスコから CIMC の .zip ファームウェア ファイルを取得します。
- TFTP サーバで、適切な .bin アップグレード ファイルを解凍します。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Firmware Management] をクリックします。

ステップ 3 [Actions] 領域で、[Install CIMC Firmware from TFTP Server] をクリックします。

ステップ 4 [Install Firmware] 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
[TFTP Server IP Address] フィールド	ファームウェア イメージが存在する TFTP サーバの IP アドレス。
[Image Path and Filename] フィールド	サーバ上のファームウェア イメージ ファイルの名前。 この名前を入力するときは、イメージ ファイルの相対パスを、TFTP ツリーの最上位からファイルの場所まで含めてください。

ステップ 5 [Install Firmware] をクリックします。

次の作業

CIMC ファームウェアをアクティブにします。

ブラウザ経由の CIMC ファームウェアのインストール

はじめる前に

- ブラウザ経由で CIMC ファームウェア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。
- シスコから CIMC の .zip ファームウェア ファイルを取得します。
- ローカル マシンで、適切な .bin アップグレード ファイルを解凍します。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブの [Firmware Management] をクリックします。
ステップ 3 [Actions] 領域で、[Install CIMC Firmware through Browser Client] をクリックします。
ステップ 4 [Install Firmware] ダイアログボックスで、[Browse] をクリックし、[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 [Install Firmware] をクリックします。

次の作業

CIMC ファームウェアをアクティブにします。

インストールされているCIMCファームウェアのアクティブ化

はじめる前に

- ファームウェアをアクティブにするには、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。
- CIMC ファームウェアをサーバにインストールします。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブの [Firmware Management] をクリックします。
ステップ 3 [Actions] 領域で、[Activate CIMC Firmware] をクリックします。
[Activate Firmware] ダイアログボックスが表示されます。
ステップ 4 [Activate Firmware] ダイアログボックスで、アクティブにするファームウェアイメージを選択します。
ステップ 5 [Activate Firmware] をクリックします。

TFTP 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。その他の BIOS のインストール方法については、『*Cisco UCS C-Series Rack-Mount Server BIOS Upgrade Guide*』を参照してください。

はじめる前に

- BIOS ファームウェア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。
- シスコから BIOS のファームウェア ファイルを取得します。
- TFTP サーバで、適切なアップグレード ファイルを解凍します。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Firmware Management] をクリックします。

ステップ 3 [Actions] 領域で、[Install BIOS Firmware from TFTP Server] をクリックします。

ステップ 4 [Install BIOS Firmware] 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
[TFTP Server IP Address] フィールド	ファームウェア イメージが存在する TFTP サーバの IP アドレス。
[Image Path and Filename] フィールド	サーバ上のファームウェア イメージ ファイルの名前。この名前を入力するときは、イメージ ファイルの相対パスを、TFTP ツリーの最上位からファイルの場所まで含めてください。

ステップ 5 [Install Firmware] をクリックします。

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。その他の BIOS のインストール方法については、『*Cisco UCS C-Series Rack-Mount Server BIOS Upgrade Guide*』を参照してください。

はじめる前に

BIOS 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。

- ブラウザ経由で BIOS ファームウェア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。
- シスコから BIOS の .zip ファームウェア ファイルを取得します。
- ローカル マシンで、適切な .bin アップグレード ファイルを解凍します。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Firmware Management] をクリックします。

ステップ 3 [Actions] 領域で、[Install BIOS Firmware through Browser Client] をクリックします。

ステップ 4 [Install BIOS Firmware] ダイアログボックスで、[Browse] をクリックし、[Choose File] ダイアログボックスを使用してインストールするファイルを選択します。

ステップ 5 [Install Firmware] をクリックします。

第 14 章

ログの表示

この章の内容は、次のとおりです。

- CIMC ログ，155 ページ
- システム イベント ログ，159 ページ

CIMC ログ

CIMC ログの表示

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [CIMC Log] をクリックします。

ステップ 3 ログの CIMC イベントごとに次の情報を確認します。

名前	説明
[Time] カラム	イベントが発生した日時。

名前	説明
[Severity] カラム	イベントの重大度。 次のいずれかになります。 • Emergency • Alert • Critical • Error • Warning • Notice • Informational • Debug
[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。
[Description] カラム	イベントの説明。
[Clear Log] ボタン	すべてのイベントをログ ファイルからクリアします。 （注） このオプションは、ユーザ ID に admin または user ユーザ ロールが割り当てられている場合にのみ使用できます。

ステップ 4 [Entries Per Page] ドロップダウン リストから、各ページに表示する CIMC イベントの数を選択します。

ステップ 5 CIMC イベントのページを前方および後方に移動するには [<Newer] および [Older>] をクリックし、リストの先頭に移動するには [<<Newest] をクリックします。
デフォルトでは、最新の CIMC イベントがリストの先頭に表示されます。

CIMC ログのクリア

はじめる前に

CIMC 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 [Navigation] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブの [CIMC Log] をクリックします。
ステップ 3 [CIMC Log] ペインで、[Clear Log] をクリックします。
ステップ 4 表示されるダイアログボックスで [OK] をクリックします。

CIMC ログしきい値の設定

CIMC 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 [Navigation] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブの [CIMC Log] をクリックします。
ステップ 3 [CIMC Log] ペインの [Logging Controls] タブをクリックします。
ステップ 4 [Local Logging] 領域で、[Minimum Severity to Report] ドロップダウン リストを使用して、CIMC 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。

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Informational
- Debug

（注） CIMC 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、[Error] を選択した場合、CIMC ログには重大度が Emergency、Alert、Critical、または Error のすべてのメッセージが含まれます。 Warning、Notice、Informational、または Debug のメッセージは表示されません。

リモート サーバへの CIMC ログの送信

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して、CIMC ログ エントリを受信できます。

はじめる前に

- リモート ホストからログを受信するようにリモート Syslog サーバを設定する必要があります。
- 認証関連のログなど、あらゆるタイプのログを受信するようにリモート Syslog サーバを設定する必要があります。
- Syslog メッセージが Syslog サーバに到達できるようにリモート Syslog サーバのファイアウォールを設定する必要があります。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [CIMC Log] をクリックします。

ステップ 3 [CIMC Log] ペインの [Logging Controls] タブをクリックします。

ステップ 4 [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	説明
[Enabled] チェックボックス	オンにすると、CIMC によって、[IP Address] フィールドで指定した Syslog サーバにログ メッセージが送信されます。
[IP Address] フィールド	CIMC ログが保存される Syslog サーバの IP アドレス。

ステップ 5 （任意） [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。

- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Informational
- Debug

（注） CIMC 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、[Error] を選択した場合、CIMC リモート ログには重大度が Emergency、Alert、Critical、または Error のすべてのメッセージが含まれます。 Warning、Notice、Informational、または Debug のメッセージは表示されません。

ステップ 6 [Save Changes] をクリックします。

システム イベント ログ

システム イベント ログの表示

手順

ステップ 1 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [System Event Log] をクリックします。

ステップ 3 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 4 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	説明
[Time] カラム	イベントが発生した日時。
[Severity] カラム	[Severity] 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。
[Description] カラム	イベントの説明。
[Clear Log] ボタン	すべてのイベントをログ ファイルからクリアします。 （注） このオプションは、ユーザ ID に admin または user ユーザ ロールが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 [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 6 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 [<Newer] および [Older>] をクリックし、リストの先頭に移動するには [<<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 [Navigation] ペインの [Server] タブをクリックします。

ステップ 2 [Server] タブの [System Event Log] をクリックします。

ステップ 3 [System Event Log] ペインで、[Clear Log] をクリックします。

ステップ 4 表示されるダイアログボックスで [OK] をクリックします。

第 15 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，161 ページ
- CIMC の再起動，163 ページ
- 破損した BIOS のリカバリ，164 ページ
- CIMC の出荷時デフォルトへのリセット，165 ページ
- CIMC 設定のエクスポートとインポート，165 ページ

テクニカル サポート データのエクスポート

TFTP 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 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Utilities] をクリックします。

ステップ 3 [Utilities] ペインの [Actions] 領域で、[Export Technical Support Data] をクリックします。

ステップ 4 [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	説明
[TFTP Server IP Address] 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 TFTP サーバの IP アドレス。

名前	説明
[Path and Filename] フィールド	サーバでサポート データを保存する必要のあるファイルの名前。 この名前を入力するときは、ファイルの相対パスを、TFTP ツリーの最上位から目的の場所まで含めてください。 （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（Cisco UCS P81E 仮想インターフェイス カードなど）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。

ステップ 5 [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 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Utilities] をクリックします。

ステップ 3 [Utilities] ペインの [Actions] 領域で、[Generate Technical Support Data for Local Download] をクリックします。

ステップ 4 [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	説明
[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、CIMC によってこのオプション ボタンが表示されます。 [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、[Actions] 領域の [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	説明
[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、CIMC 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 ファイルを新しいものと置き換えるには、このオプションを選択し、[Regenerate] をクリックします。データ収集が完了したら、[Actions] 領域の [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。
[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、CIMC 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、[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（Cisco UCS P81E 仮想インターフェイス カードなど）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。

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。

CIMC 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、非常に珍しいケースですが、サーバのトラブルシューティング時に、CIMC 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。 CIMC を再起動した後にログオフすると、CIMC 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 CIMC を再起動すると、サーバの電源は、CIMC の再起動が完了するまでオフになります。

はじめる前に

CIMC 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 [Navigation] ペインの [Admin] タブをクリックします。
ステップ 2 [Admin] タブの [Utilities] をクリックします。
ステップ 3 [Utilities] ペインの [Actions] 領域で、[Reboot CIMC] 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。

この手順以外に、破損した BIOS を回復する 3 つの方法があります。

- Cisco Host Upgrade Utility（HUU）を使用します。 これは推奨される方法です。
- CIMC CLI インターフェイスを使用します。
- サーバ モデルでサポートされている場合は、サーバのマザーボードのハードウェア ジャンパの BIOS リカバリ機能を使用します。 手順については、サーバ モデルの『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 [Navigation] ペインの [Server] タブをクリックします。
ステップ 2 [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 [Actions] 領域で、[Recover Corrupt BIOS] をクリックします。
[Recover Corrupt BIOS] ウィザードが表示されます。

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

CIMC の出荷時デフォルトへのリセット

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、非常に珍しいケースですが、サーバのトラブルシューティング時に、CIMC の出荷時デフォルトへのリセットが必要になることがあります。 これを行うと、ユーザが設定可能なすべての設定がリセットされます。

この手順は、通常のサーバ メンテナンスには含まれません。 CIMC 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。

はじめる前に

CIMC を出荷時デフォルトにリセットするには、admin 権限を持つユーザとしてログインする必要があります。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Utilities] をクリックします。

ステップ 3 [Utilities] ペインの [Actions] 領域で、[Reset CIMC 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 CIMC 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、CIMC の電源はオンになります。

CIMC 設定のエクスポートとインポート

CIMC 設定のエクスポートとインポート

CIMC 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取得し、結果の CIMC 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は、情報は管理プレーンだけから保存されます。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の機密の設定情報はエクスポートされません。

エクスポートした CIMC 設定ファイルを同じシステムに復元できます。または、別の CIMC システムにインポートできますが、その場合は、インポート システムのソフトウェア バージョンがエ

クスポートシステムのソフトウェアバージョンと同じか、設定に互換性がある必要があります。設定ファイルを別のシステムに設定テンプレートとしてインポートする場合は、IP アドレスやホスト名などの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。

CIMC 設定ファイルは、構造と要素が CIMC コマンド モードに対応している XML テキスト ファイルです。

エクスポート操作またはインポート操作を実行するときは、次の注意事項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、稼働中に実行できます。エクスポート操作はサーバまたはネットワーク トラフィックに影響しませんが、インポート操作で発生する一部の変更（IPアドレスの変更など）によって、トラフィックの中断やサーバのリブートが発生する可能性があります。
- 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。

CIMC 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または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 TFTP サーバの IP アドレスを取得します。

コンフィギュレーション 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オプションが必要な場合は、コンフィギュレーション ファイルを作成する前に、このサーバで SNMP がイネーブルになっていることを確認してください。 設定をエクスポートするときに SNMP がディセーブルになっていると、ファイルのインポート時に SNMP 値が適用されません。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Utilities] をクリックします。

ステップ 3 [Utilities] ペインの [Actions] 領域で、[Export CIMC Configuration] をクリックします。

ステップ 4 [Export CIMC 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	説明
[Export to a local file] オプション ボタン	このオプションを選択し、[Export] をクリックして、CIMC GUI を実行しているコンピュータに対してローカルなドライブに、XML 設定ファイルを保存します。 このオプションを選択すると、CIMC GUI によって、設定ファイルの保存先の場所に移動できる [Browse] ダイアログボックスが表示されます。
[Export to TFTP server] オプション ボタン	このオプションを選択して、XML 設定ファイルを TFTP サーバに保存します。 このオプションを選択すると、CIMC GUI によって次のフィールドが表示されます。 • [TFTP Server IP Address]：設定ファイルのエクスポート先の TFTP サーバの IP アドレス。 • [Path and Filename]：ファイルを TFTP サーバにエクスポートするときに CIMC によって使用されるパスおよびファイル名。

ステップ 5 [Export] をクリックします。

CIMC 設定のインポート

はじめる前に

コンフィギュレーション 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てください。 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と、現在の値がコンフィギュレーション ファイルに保存されている値で上書きされません。

手順

ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。

ステップ 2 [Admin] タブの [Utilities] をクリックします。

ステップ 3 [Utilities] ペインの [Actions] 領域で、[Import CIMC Configuration] をクリックします。

ステップ 4 [Import CIMC 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	説明
[Import from a local file] オプション ボタン	このオプションを選択し、[Import] をクリックして、CIMC GUI を実行しているコンピュータに対してローカルなドライブに保存されている XML 設定ファイルに移動します。 このオプションを選択すると、CIMC GUI によって、[File] フィールドと、インポートするファイルに移動できる [Browse] ボタンが表示されます。
[Import from TFTP server] オプション ボタン	このオプションを選択して、XML 設定ファイルを TFTP サーバからインポートします。 このオプションを選択すると、CIMC GUI によって次のフィールドが表示されます。 • [TFTP Server IP Address]：設定ファイルが存在する TFTP サーバの IP アドレス。 • [Path and Filename]：TFTP サーバ上の設定ファイルのパスおよびファイル名。

ステップ 5 [Import] をクリックします。

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。

- C200 および C210 サーバ，169 ページ
- C250 サーバ，186 ページ
- C260 サーバ，201 ページ
- C460 サーバ，217 ページ

C200 および C210 サーバ

C200 および C210 サーバの主要な BIOS パラメータ

名前	説明
[POST Error Pause] ドロップダウン リスト **set POSTErrorPause**	POST 中にサーバで重大なエラーが発生した場合の処理。 次のいずれかになります。 • [Enabled]：POST 中に重大なエラーが発生した場合、BIOS はサーバのブートを一時停止し、Error Manager を開きます。 • [Disabled]：BIOS はサーバのブートを続行します。

名前	説明
[Boot Option Retry] ドロップダウン リスト **set BootOptionRetry**	BIOS でユーザ入力を待機せずに非 EFI ベースのブート オプションを再試行するかどうか。 次のいずれかになります。 • [Enabled]：ユーザ入力を待機せずに非 EFI ベースのブート オプションを継続的に再試行します。 • [Disabled]：ユーザ入力を待機してから非 EFI ベースのブート オプションを再試行します。
[USB Boot Priority] ドロップダウン リスト **set USBBootPriority**	BIOS でサーバ ハード ドライブからのブートを試行する前に使用可能な USB デバイスからのブートを試行するかどうか。 次のいずれかになります。 • [Enabled]：サーバで USB デバイスからのブートを試行します（使用可能な場合）。 さらに、USB デバイスが検出されると、そのデバイスはブート カテゴリの一番上に配置されます。 • [Disabled]：サーバで USB デバイスを試行する前にサーバ ハード ドライブからのブートを試行します。 さらに、USB デバイスが検出されると、そのデバイスはブート カテゴリの一番下に配置されます。

C200 および C210 サーバの高度な BIOS パラメータ

[Processor Configuration] のパラメータ

名前	説明
[Intel Turbo Boost Technology] ドロップダウン リスト **set IntelTurboBoostTech**	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。 • [Disabled]：プロセッサの周波数を自動的には上げません。 • [Enabled]：必要に応じてプロセッサで Turbo Boost Technology が利用されます。

名前	説明
[Enhanced Intel Speedstep Technology] ドロップダウン リスト **set EnhancedIntelSpeedStep**	システムがプロセッサ電圧とコア周波数を調整できる Enhanced Intel SpeedStep Technology をプロセッサで使用するかどうか。 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。 • [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。 • [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。
[Intel Hyper-Threading Technology] ドロップダウン リスト **set IntelHyperThread**	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。 • [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。 • [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	説明
[Number of Enabled Cores] ドロップダウン リスト **set CoreMultiProcessing**	サーバ上の 1 つ以上の物理コアをディセーブルにできます。 次のいずれかになります。 • [All]：すべての物理コアをイネーブルにします。 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 もイネーブルになります。 • [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。 Hyper Threading をディセーブルにしてサーバで 1 つの論理プロセッサ コアのみを実行するには、[1] を選択します。 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。
[Execute Disable] ドロップダウン リスト **set ExecuteDisable**	サーバ上のメモリ領域を分類して、アプリケーション コードを実行できる場所を指定します。 この分類の結果、悪意のあるワームによってバッファへのコード挿入が試行された場合に、プロセッサはコードの実行をディセーブルにします。 この設定を使用すると、損傷、ワームの伝播、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できます。 次のいずれかになります。 • [Disabled]：プロセッサはメモリ領域を分類しません。 • [Enabled]：プロセッサは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	説明
[Intel Virtualization Technology] ドロップダウン リスト **set IntelVT**	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。 • [Disabled]：プロセッサでの仮想化を禁止します。 • [Enabled]：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 for Directed IO] ドロップダウン リスト **set IntelVTD**	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。 • [Disabled]：プロセッサでバーチャライゼーション テクノロジーを使用しません。 • [Enabled]：プロセッサでバーチャライゼーション テクノロジーを使用します。
[Intel VT-d Interrupt Remapping] ドロップダウン リスト **set InterruptRemap**	プロセッサで Intel VT-d Interrupt Remapping をサポートするかどうか。 次のいずれかになります。 • [Disabled]：プロセッサでリマッピングをサポートしません。 • [Enabled]：プロセッサで VT-d Interrupt Remapping を必要に応じて使用します。
[Intel VT-d Coherency Support] ドロップダウン リスト **set CoherencySupport**	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。 • [Disabled]：プロセッサでコヒーレンシをサポートしません。 • [Enabled]：プロセッサで VT-d Coherency を必要に応じて使用します。

名前	説明
[Intel VT-d Address Translation Services] ドロップダウン リスト **set ATS**	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。 • [Disabled]：プロセッサで ATS をサポートしません。 • [Enabled]：プロセッサで VT-d ATS を必要に応じて使用します。
[Intel VT-d PassThrough DMA] ドロップダウン リスト **set PassThroughDMA**	プロセッサで Intel VT-d Pass-through DMA をサポートするかどうか。 次のいずれかになります。 • [Disabled]：プロセッサでパススルー DMA をサポートしません。 • [Enabled]：プロセッサで VT-d Pass-through DMA を必要に応じて使用します。
[Direct Cache Access] ドロップダウン リスト **set DirectCacheAccess**	データを I/O デバイスからプロセッサ キャッシュに直接配置することによって、プロセッサで I/O パフォーマンスを向上させることができます。 この設定により、キャッシュ ミスが少なくなります。 次のいずれかになります。 • [Disabled]：I/O デバイスからのデータがプロセッサ キャッシュに直接配置されません。 • [Enabled]：I/O デバイスからのデータがプロセッサ キャッシュに直接配置されます。
[Processor C3 Report] ドロップダウン リスト **set ProcessorC3Report**	BIOS からオペレーティング システムに C3 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 C3 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。 • [Disabled]：BIOS から C3 レポートを送信しません。 • [ACPI C2]ACPI_C2：BIOS から ACPI C2 形式の C3 レポートを送信し、OS がプロセッサを電力量の少ない C3 状態に移行できるようにします。 • [ACPI C3]ACPI_C3：BIOS から ACPI C3 形式の C3 レポートを送信し、OS がプロセッサを電力量の少ない C3 状態に移行できるようにします。

名前	説明
[Processor C6 Report] ドロップダウン リスト **set ProcessorC6Report**	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。 • [Disabled]：BIOS から C6 レポートを送信しません。 • [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。
[CPU Performance] ドロップダウン リスト **set CPUPerformance**	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。 • Data Reuse Optimization • DCU Streamer Prefetcher • DCU IP Prefetcher • Hardware Prefetcher • Adjacent Cache-Line Prefetch 次のいずれかになります。 • [Enterprise]：[DCU IP Prefetcher] のみがイネーブルになります。 残りのオプションはディセーブルになります。 • [High Throughput]High_Throughput：すべてのオプションがイネーブルになります。 • [HPC]：[Data Reuse Optimization] がディセーブルになり、他のすべてのオプションはイネーブルになります。 この設定は、高パフォーマンス コンピューティングとも呼ばれます。 • [Custom]：すべてのパフォーマンス プロファイル オプションをサーバ上の BIOS セットアップから設定できます。 さらに、[Hardware Prefetcher] および [Adjacent Cache-Line Prefetch] オプションを次のフィールドで設定できます。

名前	説明
[Hardware Prefetcher] ドロップダウン リスト **set HardwarePrefetch**	Intel ハードウェア プリフェッチャで、データ ストリームと命令を、メモリから統合された第 2 レベルのキャッシュに必要に応じて取り込めるようにするかどうか。 次のいずれかになります。 • [Disabled]：ハードウェア プリフェッチャは使用されません。 • [Enabled]：キャッシュの問題が検出されたときにハードウェア プリフェッチャが使用されます。 （注） この値を指定するには、[CPU Performance]CPUPerformance を [Custom] に設定する必要があります。 [Custom] 以外の値を指定した場合、このオプションは、選択した CPU パフォーマンス プロファイルの設定で上書きされます。
[Adjacent Cache-Line Prefetch] ドロップダウン リスト **set AdjacentCacheLinePrefetch**	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。 • [Disabled]：プロセッサで必要な行のみを取得します。 • [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。 （注） この値を指定するには、[CPU Performance]CPUPerformance を [Custom] に設定する必要があります。 [Custom] 以外の値を指定した場合、このオプションは、選択した CPU パフォーマンス プロファイルの設定で上書きされます。
[CPU C State] ドロップダウン リスト **set ProcessorCcxEnable**	アイドル期間にシステムを省電力モードにすることができるかどうか。 次のいずれかになります。 • [Disabled]：システムは、アイドル状態でも高いパフォーマンスのままです。 • [Enabled]：システムは、DIMM や CPU などのシステム コンポーネントに対する電力を削減できます。 電力削減量は、[Package C State Limit] フィールド**set PackageCStateLimit** コマンドで指定します。

名前	説明
[C1E] ドロップダウン リスト **set ProcessorC1eEnable**	CPU が C1 状態になったときに最低周波数に移行するかどうか。 次のいずれかになります。 • [Disabled]：CPU は C1 状態でも最大周波数で動作し続けます。 • [Enabled]：CPU は最低周波数に移行します。 このオプションを使用すると、C1 状態で電力が最大限に節約されます。 （注） このオプションは、[CPU C State]ProcessorCcxEnable がイネーブルの場合にのみ使用します。
[OEM AESNI] ドロップダウン リスト **set OEMAESNIControl**	Advanced Encryption Standard（AES）アルゴリズムを改良する AES-NI 暗号化命令セットをサーバで使用するかどうか。 次のいずれかになります。 • [Disabled]：サーバで AES 暗号化のみを使用します。 • [Enabled]：可能な場合にサーバで AES-NI 暗号化を使用します。

[Memory Configuration] のパラメータ

名前	説明
[Select Memory RAS] ドロップダウン リスト **set SelectMemoryRAS**	サーバのメモリの信頼性、可用性、サービス性（RAS）を設定するかどうか。 次のいずれかになります。 • [Maximum Performance]Maximum_Performance：システムのパフォーマンスが最適化されます。 • [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。 • [Sparing]：一部のメモリが DIMM 障害時の使用のために予約されます。 障害が発生すると、DIMM はオフラインになり、予約済みメモリと交換されます。 このオプションを使用した場合、ミラーリングよりも冗長性が低くなりますが、サーバで実行されているプログラムに使用できるメモリの量は多くなります。

名前	説明
[NUMA Optimized] ドロップダウン リスト **set NUMAOptimize**	BIOS で NUMA をサポートするかどうか。 次のいずれかになります。 • [Disabled]：BIOS で NUMA をサポートしません。 • [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。このオプションをイネーブルにした場合は、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 インターリーブをディセーブルにする必要があります。
[Low Voltage DDR Mode] ドロップダウン リスト **set LvDDRMode**	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。 • [Power Saving Mode]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。 • [Performance Mode]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。

[Mass Storage Controller Configuration] のパラメータ

名前	説明
[Onboard SATA Controller] ドロップダウン リスト **set OnboardSATA**	プロセッサで内蔵 SATA コントローラを使用するかどうか。 次のいずれかになります。 • [Disabled]：サーバでオンボード SATA コントローラは使用されません。 • [Enabled]：プロセッサで内蔵 SATA コントローラが使用されます。

名前	説明
[SATA Mode] ドロップダウン リスト **set ConfigSATAMode**	SATA コントローラの動作モード。 次のいずれかになります。 • [AHCI]：Advanced Host Controller Interface（AHCI）がイネーブルになり、RAID がディセーブルになります。 • [Compatibility]：AHCI と RAID の両方がディセーブルになり、コントローラは IDE エミュレーション モードで動作します。 • [Enhanced]：AHCI と RAID の両方がイネーブルになります。 • [S/W RAID]：RAID がイネーブルになり、AHCI がディセーブルになります。

[Serial Port Configuration] のパラメータ

名前	説明
[Serial A Enable] ドロップダウン リスト **set Serial-PortA**	シリアル ポート A をイネーブルにするか、ディセーブルにするか。 次のいずれかになります。 • [Disabled]：シリアル ポートはディセーブルになります。 • [Enabled]：シリアル ポートはイネーブルになります。
[Serial A Address] ドロップダウン リスト **set SerialPortAAddress**	シリアル ポート A がイネーブルの場合、使用する 16 進アドレスを選択します。 次のいずれかになります。 • 3F8 • 2F8 • 3E8 • 2E8
[Serial B Enable] ドロップダウン リスト **set Serial-PortB**	シリアル ポート B をイネーブルにするか、ディセーブルにするか。 次のいずれかになります。 • [Disabled]：シリアル ポートはディセーブルになります。 • [Enabled]：シリアル ポートはイネーブルになります。

名前	説明
[Serial B Address] ドロップダウン リスト **set SerialPortBAddress**	シリアル ポート B がイネーブルの場合、使用する 16 進アドレスを選択します。 次のいずれかになります。 • 3F8 • 2F8 • 3E8 • 2E8

[USB Configuration] のパラメータ

名前	説明
[USB Controller] ドロップダウン リスト **set USBController**	プロセッサで内蔵 USB コントローラを使用するかどうか。 次のいずれかになります。 • [Disabled]：サーバで内蔵 USB コントローラは使用されません。 • [Enabled]：プロセッサで内蔵 USB コントローラが使用されます。
[Make Device Non-Bootable] ドロップダウン リスト **set MakeUSBDeviceNonBootable**	サーバを USB デバイスからブートできるかどうか。 次のいずれかになります。 • [Disabled]：サーバを USB デバイスからブートできます。 • [Enabled]：サーバを USB デバイスからブートできません。
[USB Performance Mode] ドロップダウン リスト **set USBPerformanceMode**	サーバで USB 2.0 モードと USB 1.1 モードのどちらを使用するか。 次のいずれかになります。 • [High Performance]High_Performance：サーバで EHCI（USB 2.0）コントローラがイネーブルになるため、すべての USB デバイスは USB 2.0 モードで動作します。 このオプションを使用すると、USB デバイスのパフォーマンスが最大になりますが、必要な電力量が多くなります。 • [Lower Idle Power]Lower_Idle_Power：サーバで EHCI（USB 2.0）コントローラがディセーブルになるため、すべての USB デバイスは USB 1.1 モードで動作します。 このオプションを使用すると、必要な電力量は少なくなりますが、USB デバイスのパフォーマンスが低下します。

[PCI Configuration] のパラメータ

名前	説明
[Memory Mapped I/O Above 4GB] ドロップダウン リスト **set MemoryMappedIOAbove4GB**	4 GB 以上のアドレス空間に対する 64 ビット PCI デバイスのメモリ マップ I/O をイネーブルにするか、ディセーブルにするか。 レガシー オプション ROM では、4 GB を超えるアドレスにアクセスできません。 64 ビットに対応し、レガシー オプション ROM を使用する PCI デバイスは、この設定がイネーブルの場合に正しく動作しないことがあります。 次のいずれかになります。 • [Disabled]：サーバは、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プしません。 • [Enabled]：サーバは、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プします。
[Onboard Gb NIC 1] ドロップダウン リスト **set OnboardNic1**	最初のオンボードネットワーク カード（NIC）をサーバでイネーブルにするか、ディセーブルにするか。 次のいずれかになります。 • [Disabled]：NIC 1 を使用できません。 • [Enabled]：NIC 1 を使用できます。
[Onboard Gb NIC 2] ドロップダウン リスト **set OnboardNic2**	2枚目のオンボードNICをサーバでイネーブルにするか、ディセーブルにするか。 次のいずれかになります。 • [Disabled]：NIC 2 を使用できません。 • [Enabled]：NIC 2 を使用できます。
[Onboard Gb NIC *n* ROM] ドロップダウン リスト **set OnboardNic*n*ROM**	*n* で指定されたオンボード NIC 用に組み込み PXE オプション ROM をシステムでロードするかどうか。 次のいずれかになります。 • [Disabled]：PXE オプション ROM を NIC *n* に使用できません。 • [Enabled]：PXE オプション ROM を NIC *n* に使用できます。

名前	説明
[PCIe OptionROMs] ドロップダウン リスト **set Pci-Opt-Roms**	サーバで PCIe オプション ROM 拡張スロットを使用できるかどうか。 次のいずれかになります。 • [Disabled]：PCIe オプション ROM は使用できません。 • [Enabled]：PCIe オプション ROM を使用できます。
[PCIe Slot *n* ROM] ドロップダウン リスト **set Slot*n*Disable**	*n* で指定された PCIe 拡張スロット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。 • [Disabled]：拡張スロット *n* は使用できません。 • [Enabled]：拡張スロット *n* を使用できます。
[PCIe Mezzanine Slot ROM] ドロップダウン リスト **set SlotMezzDisable**	PCIe メザニン スロット拡張 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。 • [Disabled]：メザニン スロットは使用できません。 • [Enabled]：メザニン スロットを使用できます。
[Active Video] ドロップダウン リスト **set ActiveVideo**	サーバによるビデオの表示方法。 次のいずれかになります。 • [Auto]：表示に外部グラフィック アダプタが使用されます（使用可能な場合）。 • [Onboard Device]Onboard_Device：外部グラフィック アダプタが使用可能な場合でも、常に内部グラフィックが使用されます。

C200 および C210 サーバのサーバ管理 BIOS パラメータ

名前	説明
[Assert NMI on SERR] ドロップダウン リスト **set AssertNMIOnSERR**	システム エラー（SERR）の発生時に BIOS でマスク不能割り込み（NMI）を生成してエラーをログに記録するかどうか。 次のいずれかになります。 • [Disabled]：SERR の発生時に BIOS で NMI を生成したりエラーをログに記録したりしません。 • [Enabled]：SERR の発生時に BIOS で NMI を生成し、エラーをログに記録します。 [Assert NMI on PERR]Assert_NMI_on_PERR をイネーブルにする場合は、この設定をイネーブルにする必要があります。
[Assert NMI on PERR] ドロップダウン リスト **set AssertNMIOnPERR**	プロセッサ バス パリティ エラー（PERR）の発生時に BIOS でマスク不能割り込み（NMI）を生成してエラーをログに記録するかどうか。 次のいずれかになります。 • [Disabled]：PERR の発生時に BIOS で NMI を生成したりエラーをログに記録したりしません。 • [Enabled]：PERR の発生時に BIOS で NMI を生成し、エラーをログに記録します。 この設定を使用するには、[Assert NMI on SERR]Assert_NMI_on_SERR をイネーブルにする必要があります。
[FRB2 Enable] ドロップダウン リスト **set FRB-2**	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 CIMC で FRB2 タイマーを使用するかどうか。 次のいずれかになります。 • [Disabled]：FRB2 タイマーは使用されません。 • [Enabled]：POST 中に FRB2 タイマーが開始され、必要に応じてシステムを回復するために使用されます。
[PlugNPlay BMC Detection] ドロップダウン リスト **set BMCPnP**	ACPI 対応のオペレーティング システムで BMC を自動的に検出するかどうか。 次のいずれかになります。 • [Disabled]：BMC は自動的に検出されません。 • [Enabled]：BMC は、可能な場合はいつでも自動的に検出されます。

名前	説明
[ACPI1.0 Support] ドロップダウン リスト **set ACPI10Support**	[Root System Description] テーブルの FADT の ACPI 1.0 バージョンを BIOS でパブリッシュするかどうか。 このバージョンは、ACPI 1.0 のみをサポートする OS バージョンとの互換性を保持するために必要になることがあります。 次のいずれかになります。 • [Disabled]：ACPI 1.0 バージョンはパブリッシュされません。 • [Enabled]：ACPI 1.0 バージョンはパブリッシュされます。
[Console Redirection] ドロップダウン リスト **set ConsoleRedir**	POST 中および BIOS ブート中にコンソール リダイレクションでシリアル ポートを使用できます。 BIOS のブートが終了し、オペレーティング システムがサーバの役割を果たすと、コンソール リダイレクションは無関係になり、効果がなくなります。 次のいずれかになります。 • [Disabled]：POST 中にコンソール リダイレクションは実行されません。 • [Serial Port A]Serial_Port_A：POST 中にシリアル ポート A をコンソール リダイレクション用にイネーブルにします。 （注） このオプションをイネーブルにすると、POST 中に Quiet Boot ロゴ画面の表示がディセーブルになります。
[Flow Control] ドロップダウン リスト **set FlowCtrl**	ハンドシェイク プロトコルをフロー制御に使用するかどうか。 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。 • [None]：フロー制御は使用されません。 • [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 アプリケーションの設定と一致している必要があります。

名前	説明
[Baud Rate] ドロップダウン リスト **set BaudRate**	シリアル ポートの送信速度に使用するボー レート。[Console Redirection] をディセーブルにした場合、このオプションは使用できません。 次のいずれかになります。 • [9.6k]：9600 ボー レートが使用されます。 • [19.2k]：19200 ボー レートが使用されます。 • [38.4k]：38400 ボー レートが使用されます。 • [57.6k]：57600 ボー レートが使用されます。 • [115.2k]：115200 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 アプリケーションの設定と一致している必要があります。
[Terminal Type] ドロップダウン リスト **set TerminalType**	コンソール リダイレクションに使用する文字形式のタイプ。 次のいずれかになります。 • [PC-ANSI]：PC-ANSI 端末フォントが使用されます。 • [VT100]：サポートされている vt100 ビデオ端末とその文字セットが使用されます。 • [VT100-PLUS]：サポートされている vt100-plus ビデオ端末とその文字セットが使用されます。 • [VT-UTF8]：UTF-8 文字セットのビデオ端末が使用されます。 （注） この設定は、リモート ターミナル アプリケーションの設定と一致している必要があります。
[Legacy OS Redirection] ドロップダウン リスト **set LegacyOSRedir**	DOS などのレガシー オペレーティング システムからのリダイレクションをシリアル ポートでイネーブルにするかどうか。 次のいずれかになります。 • [Disabled]：コンソール リダイレクションに対してイネーブルになっているシリアル ポートがレガシー オペレーティング システムで認識されません。 • [Enabled]：コンソール リダイレクションに対してイネーブルになっているシリアル ポートがレガシー オペレーティング システムで認識されます。

C250 サーバ

C250 サーバの主要な BIOS パラメータ

名前	説明
[POST Error Pause] ドロップダウン リスト **set POSTErrorPause**	POST 中にサーバで重大なエラーが発生した場合の処理。 次のいずれかになります。 • [Enabled]：POST 中に重大なエラーが発生した場合、BIOS はサーバのブートを一時停止し、Error Manager を開きます。 • [Disabled]：BIOS はサーバのブートを続行します。
[Boot Option Retry] ドロップダウン リスト **set BootOptionRetry**	BIOS でユーザ入力を待機せずに非 EFI ベースのブート オプションを再試行するかどうか。 次のいずれかになります。 • [Enabled]：ユーザ入力を待機せずに非 EFI ベースのブート オプションを継続的に再試行します。 • [Disabled]：ユーザ入力を待機してから非 EFI ベースのブート オプションを再試行します。
[USB Boot Priority] ドロップダウン リスト **set USBBootPriority**	BIOS でサーバ ハード ドライブからのブートを試行する前に使用可能な USB デバイスからのブートを試行するかどうか。 次のいずれかになります。 • [Enabled]：サーバで USB デバイスからのブートを試行します（使用可能な場合）。 さらに、USB デバイスが検出されると、そのデバイスはブート カテゴリの一番上に配置されます。 • [Disabled]：サーバで USB デバイスを試行する前にサーバ ハード ドライブからのブートを試行します。 さらに、USB デバイスが検出されると、そのデバイスはブート カテゴリの一番下に配置されます。

C250 サーバの高度な BIOS パラメータ

[Processor Configuration] のパラメータ

名前	説明
[Intel Turbo Boost Technology] ドロップダウン リスト **set IntelTurboBoostTech**	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。 • [Disabled]：プロセッサの周波数を自動的には上げません。 • [Enabled]：必要に応じてプロセッサで Turbo Boost Technology が利用されます。
[Enhanced Intel Speedstep Technology] ドロップダウン リスト **set EnhancedIntelSpeedStep**	システムがプロセッサ電圧とコア周波数を調整できる Enhanced Intel SpeedStep Technology をプロセッサで使用するかどうか。 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。 • [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。 • [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。

名前	説明
[Intel Hyper-Threading Technology] ドロップダウン リスト **set IntelHyperThread**	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。 • [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。 • [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。
[Number of Enabled Cores] ドロップダウン リスト **set CoreMultiProcessing**	サーバ上の 1 つ以上の物理コアをディセーブルにできます。 次のいずれかになります。 • [All]：すべての物理コアをイネーブルにします。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 もイネーブルになります。 • [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。 Hyper Threading をディセーブルにしてサーバで 1 つの論理プロセッサ コアのみを実行するには、[1] を選択します。 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	説明
[Execute Disable] ドロップダウン リスト **set ExecuteDisable**	サーバ上のメモリ領域を分類して、アプリケーション コードを実行できる場所を指定します。 この分類の結果、悪意のあるワームによってバッファへのコード挿入が試行された場合に、プロセッサはコードの実行をディセーブルにします。 この設定を使用すると、損傷、ワームの伝播、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できます。 次のいずれかになります。 • [Disabled]：プロセッサはメモリ領域を分類しません。 • [Enabled]：プロセッサは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 Virtualization Technology] ドロップダウン リスト **set IntelVT**	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。 • [Disabled]：プロセッサでの仮想化を禁止します。 • [Enabled]：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 for Directed IO] ドロップダウン リスト **set IntelVTD**	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。 • [Disabled]：プロセッサでバーチャライゼーション テクノロジーを使用しません。 • [Enabled]：プロセッサでバーチャライゼーション テクノロジーを使用します。

名前	説明
[Intel VT-d Interrupt Remapping] ドロップダウン リスト **set InterruptRemap**	プロセッサで Intel VT-d Interrupt Remapping をサポートするかどうか。 次のいずれかになります。 • [Disabled]：プロセッサでリマッピングをサポートしません。 • [Enabled]：プロセッサで VT-d Interrupt Remapping を必要に応じて使用します。
[Intel VT-d Coherency Support] ドロップダウン リスト **set CoherencySupport**	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。 • [Disabled]：プロセッサでコヒーレンシをサポートしません。 • [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 Address Translation Services] ドロップダウン リスト **set ATS**	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。 • [Disabled]：プロセッサで ATS をサポートしません。 • [Enabled]：プロセッサで VT-d ATS を必要に応じて使用します。
[Intel VT-d PassThrough DMA] ドロップダウン リスト **set PassThroughDMA**	プロセッサで Intel VT-d Pass-through DMA をサポートするかどうか。 次のいずれかになります。 • [Disabled]：プロセッサでパススルー DMA をサポートしません。 • [Enabled]：プロセッサで VT-d Pass-through DMA を必要に応じて使用します。

名前	説明
[Direct Cache Access] ドロップダウン リスト **set DirectCacheAccess**	データを I/O デバイスからプロセッサ キャッシュに直接配置することによって、プロセッサで I/O パフォーマンスを向上させることができます。 この設定により、キャッシュ ミスが少なくなります。 次のいずれかになります。 • [Disabled]：I/O デバイスからのデータがプロセッサ キャッシュに直接配置されません。 • [Enabled]：I/O デバイスからのデータがプロセッサ キャッシュに直接配置されます。
[Processor C3 Report] ドロップダウン リスト **set ProcessorC3Report**	BIOS からオペレーティング システムに C3 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 C3 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。 • [Disabled]：BIOS から C3 レポートを送信しません。 • [ACPI C2]ACPI_C2：BIOS から ACPI C2 形式の C3 レポートを送信し、OS がプロセッサを電力量の少ない C3 状態に移行できるようにします。 • [ACPI C3]ACPI_C3：BIOS から ACPI C3 形式の C3 レポートを送信し、OS がプロセッサを電力量の少ない C3 状態に移行できるようにします。
[Processor C6 Report] ドロップダウン リスト **set ProcessorC6Report**	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。 • [Disabled]：BIOS から C6 レポートを送信しません。 • [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。

名前	説明
[CPU Performance] ドロップダウン リスト **set CPUPerformance**	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。 • Data Reuse Optimization • DCU Streamer Prefetcher • DCU IP Prefetcher • Hardware Prefetcher • Adjacent Cache-Line Prefetch 次のいずれかになります。 • [Enterprise]：[DCU IP Prefetcher] のみがイネーブルになります。残りのオプションはディセーブルになります。 • [High Throughput]High_Throughput：すべてのオプションがイネーブルになります。 • [HPC]：[Data Reuse Optimization] がディセーブルになり、他のすべてのオプションはイネーブルになります。 この設定は、高パフォーマンス コンピューティングとも呼ばれます。 • [Custom]：すべてのパフォーマンス プロファイル オプションをサーバ上の BIOS セットアップから設定できます。 さらに、[Hardware Prefetcher] および [Adjacent Cache-Line Prefetch] オプションを次のフィールドで設定できます。

名前	説明
[Hardware Prefetcher] ドロップダウン リスト **set HardwarePrefetch**	Intel ハードウェア プリフェッチャで、データ ストリームと命令を、メモリから統合された第 2 レベルのキャッシュに必要に応じて取り込めるようにするかどうか。 次のいずれかになります。 • [Disabled]：ハードウェア プリフェッチャは使用されません。 • [Enabled]：キャッシュの問題が検出されたときにハードウェア プリフェッチャが使用されます。 （注） この値を指定するには、[CPU Performance]CPUPerformance を [Custom] に設定する必要があります。 [Custom] 以外の値を指定した場合、このオプションは、選択した CPU パフォーマンス プロファイルの設定で上書きされます。
[Adjacent Cache-Line Prefetch] ドロップダウン リスト **set AdjacentCacheLinePrefetch**	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。 • [Disabled]：プロセッサで必要な行のみを取得します。 • [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。 （注） この値を指定するには、[CPU Performance]CPUPerformance を [Custom] に設定する必要があります。 [Custom] 以外の値を指定した場合、このオプションは、選択した CPU パフォーマンス プロファイルの設定で上書きされます。
[CPU C State] ドロップダウン リスト **set ProcessorCcxEnable**	アイドル期間にシステムを省電力モードにすることができるかどうか。 次のいずれかになります。 • [Disabled]：システムは、アイドル状態でも高いパフォーマンスのままです。 • [Enabled]：システムは、DIMM や CPU などのシステム コンポーネントに対する電力を削減できます。 電力削減量は、[Package C State Limit] フィールド**set PackageCStateLimit** コマンドで指定します。

名前	説明
[C1E] ドロップダウン リスト **set ProcessorC1eEnable**	CPU が C1 状態になったときに最低周波数に移行するかどうか。 次のいずれかになります。 • [Disabled]：CPU は C1 状態でも最大周波数で動作し続けます。 • [Enabled]：CPU は最低周波数に移行します。 このオプションを使用すると、C1 状態で電力が最大限に節約されます。 （注） このオプションは、[CPU C State]ProcessorCcxEnable がイネーブルの場合にのみ使用します。
[Spread Spectrum] ドロップダウン リスト **set Ck410bConfigSpreadSpectrumEnable**	スペクトラム拡散は、マザーボードのクロックによって生成されたパルスを変調して、それらのパルスによって生成された EMI（電磁干渉）を少なくします。 次のいずれかになります。 • [Disabled]：サーバでスペクトラム拡散機能を使用しません。 • [Enabled]：サーバでスペクトラム拡散機能を使用します。
[OEM AESNI] ドロップダウン リスト **set OEMAESNIControl**	Advanced Encryption Standard（AES）アルゴリズムを改良する AES-NI 暗号化命令セットをサーバで使用するかどうか。 次のいずれかになります。 • [Disabled]：サーバで AES 暗号化のみを使用します。 • [Enabled]：可能な場合にサーバで AES-NI 暗号化を使用します。

[Memory Configuration] のパラメータ

名前	説明
[Select Memory RAS] ドロップダウン リスト **set SelectMemoryRAS**	サーバのメモリの信頼性、可用性、サービス性（RAS）を設定するかどうか。 次のいずれかになります。 • [Maximum Performance]Maximum_Performance：システムのパフォーマンスが最適化されます。 • [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。 • [Sparing]：一部のメモリが DIMM 障害時の使用のために予約されます。 障害が発生すると、DIMM はオフラインになり、予約済みメモリと交換されます。 このオプションを使用した場合、ミラーリングよりも冗長性が低くなりますが、サーバで実行されているプログラムに使用できるメモリの量は多くなります。
[NUMA Optimized] ドロップダウン リスト **set NUMAOptimize**	BIOS で NUMA をサポートするかどうか。 次のいずれかになります。 • [Disabled]：BIOS で NUMA をサポートしません。 • [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。 このオプションをイネーブルにした場合は、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 インターリーブをディセーブルにする必要があります。
[Low Voltage DDR Mode] ドロップダウン リスト **set LvDDRMode**	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。 • [Power Saving Mode]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。 • [Performance Mode]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。

[Serial Port Configuration] のパラメータ

名前	説明
[Serial A Enable] ドロップダウン リスト **set Serial-PortA**	シリアル ポート A をイネーブルにするか、ディセーブルにするか。 次のいずれかになります。 • [Disabled]：シリアル ポートはディセーブルになります。 • [Enabled]：シリアル ポートはイネーブルになります。
[Serial A Address] ドロップダウン リスト **set SerialPortAAddress**	シリアル ポート A がイネーブルの場合、使用する 16 進アドレスを選択します。 次のいずれかになります。 • 3F8 • 2F8 • 3E8 • 2E8

[USB Configuration] のパラメータ

名前	説明
[USB Controller] ドロップダウン リスト **set USBController**	プロセッサで内蔵 USB コントローラを使用するかどうか。 次のいずれかになります。 • [Disabled]：サーバで内蔵 USB コントローラは使用されません。 • [Enabled]：プロセッサで内蔵 USB コントローラが使用されます。
[Make Device Non-Bootable] ドロップダウン リスト **set MakeUSBDeviceNonBootable**	サーバを USB デバイスからブートできるかどうか。 次のいずれかになります。 • [Disabled]：サーバを USB デバイスからブートできます。 • [Enabled]：サーバを USB デバイスからブートできません。

[PCI Configuration] のパラメータ

名前	説明
[Memory Mapped I/O Above 4GB] ドロップダウン リスト **set MemoryMappedIOAbove4GB**	4 GB 以上のアドレス空間に対する 64 ビット PCI デバイスのメモリ マップ I/O をイネーブルにするか、ディセーブルにするか。 レガシー オプション ROM では、4 GB を超えるアドレスにアクセスできません。 64 ビットに対応し、レガシー オプション ROM を使用する PCI デバイスは、この設定がイネーブルの場合に正しく動作しないことがあります。 次のいずれかになります。 • [Disabled]：サーバは、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プしません。 • [Enabled]：サーバは、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プします。
[Onboard Gb NIC 1] ドロップダウン リスト **set OnboardNic1**	最初のオンボードネットワーク カード（NIC）をサーバでイネーブルにするか、ディセーブルにするか。 次のいずれかになります。 • [Disabled]：NIC 1 を使用できません。 • [Enabled]：NIC 1 を使用できます。
[Onboard Gb NIC 2] ドロップダウン リスト **set OnboardNic2**	2枚目のオンボードNICをサーバでイネーブルにするか、ディセーブルにするか。 次のいずれかになります。 • [Disabled]：NIC 2 を使用できません。 • [Enabled]：NIC 2 を使用できます。
[Onboard Gb NIC *n* ROM] ドロップダウン リスト **set OnboardNic*n*ROM**	*n* で指定されたオンボード NIC 用に組み込み PXE オプション ROM をシステムでロードするかどうか。 次のいずれかになります。 • [Disabled]：PXE オプション ROM を NIC *n* に使用できません。 • [Enabled]：PXE オプション ROM を NIC *n* に使用できます。

名前	説明
[PCIe OptionROMs] ドロップダウン リスト **set Pci-Opt-Roms**	サーバで PCIe オプション ROM 拡張スロットを使用できるかどうか。 次のいずれかになります。 • [Disabled]：PCIe オプション ROM は使用できません。 • [Enabled]：PCIe オプション ROM を使用できます。
[PCIe Slot *n* ROM] ドロップダウン リスト **set Slot*n*Disable**	*n* で指定された PCIe 拡張スロット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。 • [Disabled]：拡張スロット *n* は使用できません。 • [Enabled]：拡張スロット *n* を使用できます。
[Active Video] ドロップダウン リスト **set ActiveVideo**	サーバによるビデオの表示方法。 次のいずれかになります。 • [Auto]：表示に外部グラフィック アダプタが使用されます（使用可能な場合）。 • [Onboard Device]Onboard_Device：外部グラフィック アダプタが使用可能な場合でも、常に内部グラフィックが使用されます。

C250 サーバのサーバ管理 BIOS パラメータ

名前	説明
[Assert NMI on SERR] ドロップダウン リスト **set AssertNMIOnSERR**	システム エラー（SERR）の発生時に BIOS でマスク不能割り込み（NMI）を生成してエラーをログに記録するかどうか。 次のいずれかになります。 • [Disabled]：SERR の発生時に BIOS で NMI を生成したりエラーをログに記録したりしません。 • [Enabled]：SERR の発生時に BIOS で NMI を生成し、エラーをログに記録します。 [Assert NMI on PERR]Assert_NMI_on_PERR をイネーブルにする場合は、この設定をイネーブルにする必要があります。

名前	説明
[Assert NMI on PERR] ドロップダウン リスト **set AssertNMIOnPERR**	プロセッサ バス パリティ エラー（PERR）の発生時に BIOS でマスク不能割り込み（NMI）を生成してエラーをログに記録するかどうか。 次のいずれかになります。 • [Disabled]：PERR の発生時に BIOS で NMI を生成したりエラーをログに記録したりしません。 • [Enabled]：PERR の発生時に BIOS で NMI を生成し、エラーをログに記録します。 この設定を使用するには、[Assert NMI on SERR]Assert_NMI_on_SERR をイネーブルにする必要があります。
[FRB2 Enable] ドロップダウン リスト **set FRB-2**	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 CIMC で FRB2 タイマーを使用するかどうか。 次のいずれかになります。 • [Disabled]：FRB2 タイマーは使用されません。 • [Enabled]：POST 中に FRB2 タイマーが開始され、必要に応じてシステムを回復するために使用されます。
[PlugNPlay BMC Detection] ドロップダウン リスト **set BMCPnP**	ACPI 対応のオペレーティング システムで BMC を自動的に検出するかどうか。 次のいずれかになります。 • [Disabled]：BMC は自動的に検出されません。 • [Enabled]：BMC は、可能な場合はいつでも自動的に検出されます。
[ACPI1.0 Support] ドロップダウン リスト **set ACPI10Support**	[Root System Description] テーブルの FADT の ACPI 1.0 バージョンを BIOS でパブリッシュするかどうか。 このバージョンは、ACPI 1.0 のみをサポートする OS バージョンとの互換性を保持するために必要になることがあります。 次のいずれかになります。 • [Disabled]：ACPI 1.0 バージョンはパブリッシュされません。 • [Enabled]：ACPI 1.0 バージョンはパブリッシュされます。

名前	説明
[Console Redirection] ドロップダウン リスト **set ConsoleRedir**	POST 中および BIOS ブート中にコンソール リダイレクションでシリアル ポートを使用できます。 BIOS のブートが終了し、オペレーティング システムがサーバの役割を果たすと、コンソール リダイレクションは無関係になり、効果がなくなります。 次のいずれかになります。 • [Disabled]：POST 中にコンソール リダイレクションは実行されません。 • [Serial Port A]Serial_Port_A：POST 中にシリアル ポート A をコンソール リダイレクション用にイネーブルにします。 （注） このオプションをイネーブルにすると、POST 中に Quiet Boot ロゴ画面の表示がディセーブルになります。
[Flow Control] ドロップダウン リスト **set FlowCtrl**	ハンドシェイク プロトコルをフロー制御に使用するかどうか。 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。 • [None]：フロー制御は使用されません。 • [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 アプリケーションの設定と一致している必要があります。
[Baud Rate] ドロップダウン リスト **set BaudRate**	シリアル ポートの送信速度に使用するボー レート。 [Console Redirection] をディセーブルにした場合、このオプションは使用できません。 次のいずれかになります。 • [9.6k]：9600 ボー レートが使用されます。 • [19.2k]：19200 ボー レートが使用されます。 • [38.4k]：38400 ボー レートが使用されます。 • [57.6k]：57600 ボー レートが使用されます。 • [115.2k]：115200 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 アプリケーションの設定と一致している必要があります。

名前	説明
[Terminal Type] ドロップダウン リスト **set TerminalType**	コンソール リダイレクションに使用する文字形式のタイプ。 次のいずれかになります。 • [PC-ANSI]：PC-ANSI 端末フォントが使用されます。 • [VT100]：サポートされている vt100 ビデオ端末とその文字セットが使用されます。 • [VT100-PLUS]：サポートされている vt100-plus ビデオ端末とその文字セットが使用されます。 • [VT-UTF8]：UTF-8 文字セットのビデオ端末が使用されます。 （注） この設定は、リモート ターミナル アプリケーションの設定と一致している必要があります。
[Legacy OS Redirection] ドロップダウン リスト **set LegacyOSRedir**	DOS などのレガシー オペレーティング システムからのリダイレクションをシリアル ポートでイネーブルにするかどうか。 次のいずれかになります。 • [Disabled]：コンソール リダイレクションに対してイネーブルになっているシリアル ポートがレガシー オペレーティング システムで認識されません。 • [Enabled]：コンソール リダイレクションに対してイネーブルになっているシリアル ポートがレガシー オペレーティング システムで認識されます。

C260 サーバ

C260 サーバの主要な BIOS パラメータ

名前	説明
[POST Error Pause] ドロップダウン リスト **set POSTErrorPause**	POST 中にサーバで重大なエラーが発生した場合の処理。 次のいずれかになります。 • [Enabled]：POST 中に重大なエラーが発生した場合、BIOS はサーバのブートを一時停止し、Error Manager を開きます。 • [Disabled]：BIOS はサーバのブートを続行します。

名前	説明
[Boot Option Retry] ドロップダウン リスト **set BootOptionRetry**	BIOS でユーザ入力を待機せずに非 EFI ベースのブート オプションを再試行するかどうか。 次のいずれかになります。 • [Enabled]：ユーザ入力を待機せずに非 EFI ベースのブート オプションを継続的に再試行します。 • [Disabled]：ユーザ入力を待機してから非 EFI ベースのブート オプションを再試行します。

C260 サーバの高度な BIOS パラメータ

[Processor Configuration] のパラメータ

名前	説明
[Intel Turbo Boost Technology] ドロップダウン リスト **set IntelTurboBoostTech**	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。 • [Disabled]：プロセッサの周波数を自動的には上げません。 • [Enabled]：必要に応じてプロセッサで Turbo Boost Technology が利用されます。

名前	説明
[Enhanced Intel Speedstep Technology] ドロップダウン リスト **set EnhancedIntelSpeedStep**	システムがプロセッサ電圧とコア周波数を調整できる Enhanced Intel SpeedStep Technology をプロセッサで使用するかどうか。 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。 • [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。 • [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。
[Intel Hyper-Threading Technology] ドロップダウン リスト **set IntelHyperThread**	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。 • [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。 • [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	説明
[Number of Enabled Cores] ドロップダウン リスト **set CoreMultiProcessing**	サーバ上の 1 つ以上の物理コアをディセーブルにできます。 次のいずれかになります。 • [All]：すべての物理コアをイネーブルにします。 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 もイネーブルになります。 • [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。 Hyper Threading をディセーブルにしてサーバで 1 つの論理プロセッサ コアのみを実行するには、[1] を選択します。 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。
[Execute Disable] ドロップダウン リスト **set ExecuteDisable**	サーバ上のメモリ領域を分類して、アプリケーション コードを実行できる場所を指定します。 この分類の結果、悪意のあるワームによってバッファへのコード挿入が試行された場合に、プロセッサはコードの実行をディセーブルにします。 この設定を使用すると、損傷、ワームの伝播、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できます。 次のいずれかになります。 • [Disabled]：プロセッサはメモリ領域を分類しません。 • [Enabled]：プロセッサは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	説明
[Intel Virtualization Technology] ドロップダウン リスト **set IntelVT**	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。 • [Disabled]：プロセッサでの仮想化を禁止します。 • [Enabled]：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 for Directed IO] ドロップダウン リスト **set IntelVTD**	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。 • [Disabled]：プロセッサでバーチャライゼーション テクノロジーを使用しません。 • [Enabled]：プロセッサでバーチャライゼーション テクノロジーを使用します。
[Intel VT-d Interrupt Remapping] ドロップダウン リスト **set InterruptRemap**	プロセッサで Intel VT-d Interrupt Remapping をサポートするかどうか。 次のいずれかになります。 • [Disabled]：プロセッサでリマッピングをサポートしません。 • [Enabled]：プロセッサで VT-d Interrupt Remapping を必要に応じて使用します。
[Intel VT-d Coherency Support] ドロップダウン リスト **set CoherencySupport**	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。 • [Disabled]：プロセッサでコヒーレンシをサポートしません。 • [Enabled]：プロセッサで VT-d Coherency を必要に応じて使用します。

名前	説明
[Intel VT-d Address Translation Services] ドロップダウン リスト **set ATS**	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。 • [Disabled]：プロセッサで ATS をサポートしません。 • [Enabled]：プロセッサで VT-d ATS を必要に応じて使用します。
[Intel VT-d PassThrough DMA] ドロップダウン リスト **set PassThroughDMA**	プロセッサで Intel VT-d Pass-through DMA をサポートするかどうか。 次のいずれかになります。 • [Disabled]：プロセッサでパススルー DMA をサポートしません。 • [Enabled]：プロセッサで VT-d Pass-through DMA を必要に応じて使用します。
[Direct Cache Access] ドロップダウン リスト **set DirectCacheAccess**	データを I/O デバイスからプロセッサ キャッシュに直接配置することによって、プロセッサで I/O パフォーマンスを向上させることができます。 この設定により、キャッシュ ミスが少なくなります。 次のいずれかになります。 • [Disabled]：I/O デバイスからのデータがプロセッサ キャッシュに直接配置されません。 • [Enabled]：I/O デバイスからのデータがプロセッサ キャッシュに直接配置されます。
[Processor C3 Report] ドロップダウン リスト **set ProcessorC3Report**	BIOS からオペレーティング システムに C3 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 C3 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。 • [Disabled]：BIOS から C3 レポートを送信しません。 • [ACPI C2]ACPI_C2：BIOS から ACPI C2 形式の C3 レポートを送信し、OS がプロセッサを電力量の少ない C3 状態に移行できるようにします。 • [ACPI C3]ACPI_C3：BIOS から ACPI C3 形式の C3 レポートを送信し、OS がプロセッサを電力量の少ない C3 状態に移行できるようにします。

名前	説明
[Processor C6 Report] ドロップダウン リスト **set ProcessorC6Report**	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。 • [Disabled]：BIOS から C6 レポートを送信しません。 • [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。

名前	説明
[Package C State Limit] ドロップダウン リスト **set PackageCStateLimit**	アイドル状態のサーバ コンポーネントが使用できる電力量。 次のいずれかになります。 • [C0 state]C0_state：すべてのサーバ コンポーネントに常にフルパワーが供給されます。 このオプションを使用すると、最高レベルのパフォーマンスが維持されますが、必要な電力量は最も多くなります。 • [C1 state]C1_state：CPU がアイドル状態の場合、電力消費量が若干少なくなります。 このオプションを使用すると、C0 よりも必要な電力量は少なくなり、サーバはすぐに高パフォーマンス モードに戻ることができます。 • [C3 state]C3_state：CPU がアイドル状態の場合、C1 オプションのときよりもさらに電力消費量が少なくなります。 このオプションを使用すると、C1 または C0 よりも必要な電力が少なくなりますが、サーバが高パフォーマンス モードに戻るまでの時間が若干長くなります。 • [C6 state]C6_state：CPU がアイドル状態の場合、C3 オプションのときよりもさらに電力消費量が少なくなります。 このオプションを使用すると、C0、C1、または C3 よりも電力量が節約されますが、サーバがフルパワーに戻るまでにパフォーマンス上の問題が発生する可能性があります。 • [C7 state]C7_state：CPU がアイドル状態の場合、コンポーネントで利用できる電力量が最小になります。 このオプションを使用すると、電力量が最大限に節約されますが、サーバが高パフォーマンス モードに戻るまでの時間が最も長くなります。 • [No Limit]No_Limit：サーバは使用可能などの C 状態にもなることができます。 （注） このオプションは、[CPU C State] がイネーブルの場合にのみ使用します。

名前	説明
[CPU C State] ドロップダウン リスト **set ProcessorCcxEnable**	アイドル期間にシステムを省電力モードにすることができるかどうか。 次のいずれかになります。 • [Disabled]：システムは、アイドル状態でも高いパフォーマンスのままです。 • [Enabled]：システムは、DIMM や CPU などのシステム コンポーネントに対する電力を削減できます。電力削減量は、[Package C State Limit] フィールド**set PackageCStateLimit** コマンドで指定します。
[C1E] ドロップダウン リスト **set ProcessorC1eEnable**	CPU が C1 状態になったときに最低周波数に移行するかどうか。 次のいずれかになります。 • [Disabled]：CPU は C1 状態でも最大周波数で動作し続けます。 • [Enabled]：CPU は最低周波数に移行します。 このオプションを使用すると、C1 状態で電力が最大限に節約されます。 （注） このオプションは、[CPU C State]ProcessorCcxEnable がイネーブルの場合にのみ使用します。

[Memory Configuration] のパラメータ

名前	説明
[Select Memory RAS] ドロップダウン リスト **set SelectMemoryRAS**	サーバのメモリの信頼性、可用性、サービス性（RAS）を設定するかどうか。 次のいずれかになります。 • [Maximum Performance]Maximum_Performance：システムのパフォーマンスが最適化されます。 • [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。 • [Sparing]：一部のメモリが DIMM 障害時の使用のために予約されます。 障害が発生すると、DIMM はオフラインになり、予約済みメモリと交換されます。 このオプションを使用した場合、ミラーリングよりも冗長性が低くなりますが、サーバで実行されているプログラムに使用できるメモリの量は多くなります。

名前	説明
[NUMA Optimized] ドロップダウン リスト **set NUMAOptimize**	BIOS で NUMA をサポートするかどうか。 次のいずれかになります。 • [Disabled]：BIOS で NUMA をサポートしません。 • [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。このオプションをイネーブルにした場合は、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 インターリーブをディセーブルにする必要があります。
[Sparing Mode] ドロップダウン リスト **set SparingMode**	CIMC で使用するスペア モード。 次のいずれかになります。 • [Rank Sparing]Rank_Sparing：スペア メモリはランク レベルで割り当てられます。 • [DIMM Sparing]：スペア メモリは DIMM レベルで割り当てられます。 （注） このオプションは、[Select Memory RAS]set SelectMemoryRAS が [Sparing] に設定されている場合にのみ使用します。
[Mirroring Mode] ドロップダウン リスト **set MirroringMode**	1 つのメモリ ライザーが別のメモリ ライザーとミラーリングされる統合メモリ コントローラ（IMC）間でのミラーリングがサポートされます。 次のいずれかになります。 • [Intersocket]：各 IMC が 2 つのソケット間でミラーリングされます。 • [Intrasocket]：1 つの IMC が同じソケット内の別の IMC とミラーリングされます。 （注） このオプションは、[Select Memory RAS]SelectMemoryRAS が [Mirroring] に設定されている場合にのみ使用します。

名前	説明
[Patrol Scrub] ドロップダウン リスト **set PatrolScrub**	サーバ上のメモリの未使用部分でも、シングル ビット メモリ エラーをシステムでアクティブに検索して修正するかどうか。 次のいずれかになります。 • [Disabled]：CPU によってメモリ アドレスの読み取りまたは書き込みが行われる場合にのみ、システムでメモリの ECC エラーを確認します。 • [Enabled]：システムで定期的にメモリの読み取りおよび書き込みを行って ECC エラーを検索します。 エラーが見つかった場合は修正を試みます。 このオプションによって、シングル ビット エラーをマルチビット エラーになる前に修正できますが、パトロール スクラビング処理の実行時にパフォーマンスが低下する可能性があります。
[Patrol Scrub Interval] ドロップダウン リスト **set PatrolScrubDuration**	パトロール スクラビング処理によるメモリ アクセスの時間間隔を制御します。 間隔が短いほど、メモリのスクラビング処理の頻度が高くなりますが、必要なメモリ帯域幅が多くなります。 5 ～ 23 の範囲の値を選択します。 デフォルト値は、8 です。 （注） このオプションは、[Patrol Scrub] がイネーブルの場合にのみ使用します。
[CKE Low Policy] ドロップダウン リスト **set CKELowPolicy**	DIMM 省電力モード ポリシーを制御します。 次のいずれかになります。 • [Disabled]：DIMM は省電力モードになりません。 • [Slow]：DIMM は省電力モードになる可能性がありますが、要件が高くなります。 したがって、DIMM が省電力モードになる頻度は低くなります。 • [Fast]：DIMM は頻繁に省電力モードになります。 • [Auto]：BIOS は、DIMM の設定に基づいて DIMM が省電力モードになるタイミングを制御します。

[Serial Port Configuration] のパラメータ

名前	説明
[Serial A Enable] ドロップダウン リスト **set Serial-PortA**	シリアル ポート A をイネーブルにするか、ディセーブルにするか。 次のいずれかになります。 • [Disabled]：シリアル ポートはディセーブルになります。 • [Enabled]：シリアル ポートはイネーブルになります。

[USB Configuration] のパラメータ

名前	説明
[Make Device Non-Bootable] ドロップダウン リスト **set MakeUSBDeviceNonBootable**	サーバを USB デバイスからブートできるかどうか。 次のいずれかになります。 • [Disabled]：サーバを USB デバイスからブートできます。 • [Enabled]：サーバを USB デバイスからブートできません。

[PCI Configuration] のパラメータ

名前	説明
[Memory Mapped I/O Above 4GB] ドロップダウン リスト **set MemoryMappedIOAbove4GB**	4 GB 以上のアドレス空間に対する 64 ビット PCI デバイスのメモリ マップ I/O をイネーブルにするか、ディセーブルにするか。 レガシー オプション ROM では、4 GB を超えるアドレスにアクセスできません。 64 ビットに対応し、レガシー オプション ROM を使用する PCI デバイスは、この設定がイネーブルの場合に正しく動作しないことがあります。 次のいずれかになります。 • [Disabled]：サーバは、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プしません。 • [Enabled]：サーバは、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プします。

名前	説明
[Onboard NIC *n* ROM] ドロップダウン リスト **set OnboardNic*n*ROM**	*n* で指定されたオンボード NIC 用に組み込み PXE オプション ROM をシステムでロードするかどうか。 次のいずれかになります。 • [Disabled]：PXE オプション ROM を NIC *n* に使用できません。 • [Enabled]：PXE オプション ROM を NIC *n* に使用できます。
[PCIe OptionROMs] ドロップダウン リスト **set Pci-Opt-Roms**	サーバで PCIe オプション ROM 拡張スロットを使用できるかどうか。 次のいずれかになります。 • [Disabled]：PCIe オプション ROM は使用できません。 • [Enabled]：PCIe オプション ROM を使用できます。
[PCIe Slot *n* ROM] ドロップダウン リスト **set Slot*n*Disable**	*n* で指定された PCIe 拡張スロット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。 • [Disabled]：拡張スロット *n* は使用できません。 • [Enabled]：拡張スロット *n* を使用できます。

C260 サーバのサーバ管理 BIOS パラメータ

名前	説明
[Assert NMI on SERR] ドロップダウン リスト **set AssertNMIOnSERR**	システム エラー（SERR）の発生時に BIOS でマスク不能割り込み（NMI）を生成してエラーをログに記録するかどうか。 次のいずれかになります。 • [Disabled]：SERR の発生時に BIOS で NMI を生成したりエラーをログに記録したりしません。 • [Enabled]：SERR の発生時に BIOS で NMI を生成し、エラーをログに記録します。 [Assert NMI on PERR]Assert_NMI_on_PERR をイネーブルにする場合は、この設定をイネーブルにする必要があります。

名前	説明
[Assert NMI on PERR] ドロップダウン リスト **set AssertNMIOnPERR**	プロセッサ バス パリティ エラー（PERR）の発生時に BIOS でマスク不能割り込み（NMI）を生成してエラーをログに記録するかどうか。 次のいずれかになります。 • [Disabled]：PERR の発生時に BIOS で NMI を生成したりエラーをログに記録したりしません。 • [Enabled]：PERR の発生時に BIOS で NMI を生成し、エラーをログに記録します。 この設定を使用するには、[Assert NMI on SERR]Assert_NMI_on_SERR をイネーブルにする必要があります。
[Console Redirection] ドロップダウン リスト **set ConsoleRedir**	POST 中および BIOS ブート中にコンソール リダイレクションでシリアル ポートを使用できます。 BIOS のブートが終了し、オペレーティング システムがサーバの役割を果たすと、コンソール リダイレクションは無関係になり、効果がなくなります。 次のいずれかになります。 • [Disabled]：POST 中にコンソール リダイレクションは実行されません。 • [Serial Port A]Serial_Port_A：POST 中にシリアル ポート A をコンソール リダイレクション用にイネーブルにします。 （注） このオプションをイネーブルにすると、POST 中に Quiet Boot ロゴ画面の表示がディセーブルになります。
[Flow Control] ドロップダウン リスト **set FlowCtrl**	ハンドシェイク プロトコルをフロー制御に使用するかどうか。 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。 • [None]：フロー制御は使用されません。 • [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 アプリケーションの設定と一致している必要があります。

名前	説明
[Baud Rate] ドロップダウン リスト **set BaudRate**	シリアル ポートの送信速度に使用するボー レート。[Console Redirection] をディセーブルにした場合、このオプションは使用できません。 次のいずれかになります。 • [9.6k]：9600 ボー レートが使用されます。 • [19.2k]：19200 ボー レートが使用されます。 • [38.4k]：38400 ボー レートが使用されます。 • [57.6k]：57600 ボー レートが使用されます。 • [115.2k]：115200 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 アプリケーションの設定と一致している必要があります。
[Terminal Type] ドロップダウン リスト **set TerminalType**	コンソール リダイレクションに使用する文字形式のタイプ。 次のいずれかになります。 • [PC-ANSI]：PC-ANSI 端末フォントが使用されます。 • [VT100]：サポートされている vt100 ビデオ端末とその文字セットが使用されます。 • [VT100-PLUS]：サポートされている vt100-plus ビデオ端末とその文字セットが使用されます。 • [VT-UTF8]：UTF-8 文字セットのビデオ端末が使用されます。 （注） この設定は、リモート ターミナル アプリケーションの設定と一致している必要があります。

名前	説明
[OS Boot Watchdog Timer Timeout] ドロップダウン リスト **set OSBootWatchdogTimerTimeOut**	BIOS でウォッチドッグ タイマーの設定に使用するタイムアウト値。 次のいずれかになります。 • [5 Minutes]5_Minutes：ウォッチドッグ タイマーは、OS のブートが開始されてから 5 分後に期限が切れます。 • [10 Minutes]10_Minutes：ウォッチドッグ タイマーは、OS のブートが開始されてから 10 分後に期限が切れます。 • [15 Minutes]15_Minutes：ウォッチドッグ タイマーは、OS のブートが開始されてから 15 分後に期限が切れます。 • [20 Minutes]20_Minutes：ウォッチドッグ タイマーは、OS のブートが開始されてから 20 分後に期限が切れます。 （注） このオプションは、[OS Boot Watchdog Timer] をイネーブルにした場合にのみ適用されます。
[OS Boot Watchdog Policy] ドロップダウン リスト **set OSBootWatchdogTimerPolicy**	ウォッチドッグ タイマーの期限が切れた場合に実行されるアクション。 次のいずれかになります。 • [Power Off]Power_Off：OS のブート中にウォッチドッグ タイマーの期限が切れた場合、サーバの電源がオフになります。 • [Reset]：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、サーバはリセットされます。 （注） このオプションは、[OS Boot Watchdog Timer] をイネーブルにした場合にのみ適用されます。
[Legacy OS Redirection] ドロップダウン リスト **set LegacyOSRedir**	DOS などのレガシー オペレーティング システムからのリダイレクションをシリアル ポートでイネーブルにするかどうか。 次のいずれかになります。 • [Disabled]：コンソール リダイレクションに対してイネーブルになっているシリアル ポートがレガシー オペレーティング システムで認識されません。 • [Enabled]：コンソール リダイレクションに対してイネーブルになっているシリアル ポートがレガシー オペレーティング システムで認識されます。

名前	説明
[OS Boot Watchdog Timer] ドロップダウン リスト **set OSBootWatchdogTimer**	BIOS で指定されたタイムアウト値を使用してウォッチドッグ タイマーをプログラミングするかどうか。 次のいずれかになります。 • [Disabled]：サーバのブートにかかる時間を追跡するためにウォッチドッグ タイマーは使用されません。 • [Enabled]：サーバのブートにかかる時間を追跡するためにウォッチドッグ タイマーが使用されます。サーバのブートが指定された時間内に完了しない場合: [OS Boot Watchdog Timer Timeout] フィールドで指定された時間内に完了しない場合は、CIMC によってエラーがログに記録され、[OS Boot Watchdog Policy] フィールドで指定されたアクションが実行されます。**set OSBootWatchdogTimerTimeout** コマンドで指定された時間内に完了しない場合は、CIMC によってエラーがログに記録され、**set OSBootWatchdogTimerPolicy** コマンドで指定されたアクションが実行されます。

C460 サーバ

C460 サーバの主要な BIOS パラメータ

名前	説明
[POST Error Pause] ドロップダウン リスト **set POSTErrorPause**	POST 中にサーバで重大なエラーが発生した場合の処理。 次のいずれかになります。 • [Enabled]：POST 中に重大なエラーが発生した場合、BIOS はサーバのブートを一時停止し、Error Manager を開きます。 • [Disabled]：BIOS はサーバのブートを続行します。

名前	説明
[Boot Option Retry] ドロップダウン リスト **set BootOptionRetry**	BIOS でユーザ入力を待機せずに非 EFI ベースのブート オプションを再試行するかどうか。 次のいずれかになります。 • [Enabled]：ユーザ入力を待機せずに非 EFI ベースのブート オプションを継続的に再試行します。 • [Disabled]：ユーザ入力を待機してから非 EFI ベースのブート オプションを再試行します。

C460 サーバの高度な BIOS パラメータ

[Processor Configuration] のパラメータ

名前	説明
[Intel Turbo Boost Technology] ドロップダウン リスト **set IntelTurboBoostTech**	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。 • [Disabled]：プロセッサの周波数を自動的には上げません。 • [Enabled]：必要に応じてプロセッサで Turbo Boost Technology が利用されます。

名前	説明
[Enhanced Intel Speedstep Technology] ドロップダウン リスト **set EnhancedIntelSpeedStep**	システムがプロセッサ電圧とコア周波数を調整できる Enhanced Intel SpeedStep Technology をプロセッサで使用するかどうか。 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。 • [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。 • [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。
[Intel Hyper-Threading Technology] ドロップダウン リスト **set IntelHyperThread**	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。 • [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。 • [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	説明
[Number of Enabled Cores] ドロップダウン リスト **set CoreMultiProcessing**	サーバ上の 1 つ以上の物理コアをディセーブルにできます。 次のいずれかになります。 • [All]：すべての物理コアをイネーブルにします。 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 もイネーブルになります。 • [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。 Hyper Threading をディセーブルにしてサーバで 1 つの論理プロセッサ コアのみを実行するには、[1] を選択します。 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。
[Execute Disable] ドロップダウン リスト **set ExecuteDisable**	サーバ上のメモリ領域を分類して、アプリケーション コードを実行できる場所を指定します。 この分類の結果、悪意のあるワームによってバッファへのコード挿入が試行された場合に、プロセッサはコードの実行をディセーブルにします。 この設定を使用すると、損傷、ワームの伝播、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できます。 次のいずれかになります。 • [Disabled]：プロセッサはメモリ領域を分類しません。 • [Enabled]：プロセッサは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	説明
[Intel Virtualization Technology] ドロップダウン リスト **set IntelVT**	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。 • [Disabled]：プロセッサでの仮想化を禁止します。 • [Enabled]：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 for Directed IO] ドロップダウン リスト **set IntelVTD**	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。 • [Disabled]：プロセッサでバーチャライゼーション テクノロジーを使用しません。 • [Enabled]：プロセッサでバーチャライゼーション テクノロジーを使用します。
[Intel VT-d Interrupt Remapping] ドロップダウン リスト **set InterruptRemap**	プロセッサで Intel VT-d Interrupt Remapping をサポートするかどうか。 次のいずれかになります。 • [Disabled]：プロセッサでリマッピングをサポートしません。 • [Enabled]：プロセッサで VT-d Interrupt Remapping を必要に応じて使用します。
[Intel VT-d Coherency Support] ドロップダウン リスト **set CoherencySupport**	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。 • [Disabled]：プロセッサでコヒーレンシをサポートしません。 • [Enabled]：プロセッサで VT-d Coherency を必要に応じて使用します。

名前	説明
[Intel VT-d Address Translation Services] ドロップダウン リスト **set ATS**	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。 • [Disabled]：プロセッサで ATS をサポートしません。 • [Enabled]：プロセッサで VT-d ATS を必要に応じて使用します。
[Intel VT-d PassThrough DMA] ドロップダウン リスト **set PassThroughDMA**	プロセッサで Intel VT-d Pass-through DMA をサポートするかどうか。 次のいずれかになります。 • [Disabled]：プロセッサでパススルー DMA をサポートしません。 • [Enabled]：プロセッサで VT-d Pass-through DMA を必要に応じて使用します。
[Direct Cache Access] ドロップダウン リスト **set DirectCacheAccess**	データを I/O デバイスからプロセッサ キャッシュに直接配置することによって、プロセッサで I/O パフォーマンスを向上させることができます。 この設定により、キャッシュ ミスが少なくなります。 次のいずれかになります。 • [Disabled]：I/O デバイスからのデータがプロセッサ キャッシュに直接配置されません。 • [Enabled]：I/O デバイスからのデータがプロセッサ キャッシュに直接配置されます。
[Processor C3 Report] ドロップダウン リスト **set ProcessorC3Report**	BIOS からオペレーティング システムに C3 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 C3 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。 • [Disabled]：BIOS から C3 レポートを送信しません。 • [ACPI C2]ACPI_C2：BIOS から ACPI C2 形式の C3 レポートを送信し、OS がプロセッサを電力量の少ない C3 状態に移行できるようにします。 • [ACPI C3]ACPI_C3：BIOS から ACPI C3 形式の C3 レポートを送信し、OS がプロセッサを電力量の少ない C3 状態に移行できるようにします。

名前	説明
[Processor C6 Report] ドロップダウン リスト **set ProcessorC6Report**	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。 • [Disabled]：BIOS から C6 レポートを送信しません。 • [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。

名前	説明
[Package C State Limit] ドロップダウン リスト **set PackageCStateLimit**	アイドル状態のサーバ コンポーネントが使用できる電力量。 次のいずれかになります。 • [C0 state]C0_state：すべてのサーバ コンポーネントに常にフルパワーが供給されます。 このオプションを使用すると、最高レベルのパフォーマンスが維持されますが、必要な電力量は最も多くなります。 • [C1 state]C1_state：CPU がアイドル状態の場合、電力消費量が若干少なくなります。 このオプションを使用すると、C0 よりも必要な電力量は少なくなり、サーバはすぐに高パフォーマンス モードに戻ることができます。 • [C3 state]C3_state：CPU がアイドル状態の場合、C1 オプションのときよりもさらに電力消費量が少なくなります。 このオプションを使用すると、C1 または C0 よりも必要な電力が少なくなりますが、サーバが高パフォーマンス モードに戻るまでの時間が若干長くなります。 • [C6 state]C6_state：CPU がアイドル状態の場合、C3 オプションのときよりもさらに電力消費量が少なくなります。 このオプションを使用すると、C0、C1、または C3 よりも電力量が節約されますが、サーバがフルパワーに戻るまでにパフォーマンス上の問題が発生する可能性があります。 • [C7 state]C7_state：CPU がアイドル状態の場合、コンポーネントで利用できる電力量が最小になります。 このオプションを使用すると、電力量が最大限に節約されますが、サーバが高パフォーマンス モードに戻るまでの時間が最も長くなります。 • [No Limit]No_Limit：サーバは使用可能などの C 状態にもなることができます。 （注） このオプションは、[CPU C State] がイネーブルの場合にのみ使用します。

名前	説明
[CPU C State] ドロップダウン リスト **set ProcessorCcxEnable**	アイドル期間にシステムを省電力モードにすることができるかどうか。 次のいずれかになります。 • [Disabled]：システムは、アイドル状態でも高いパフォーマンスのままです。 • [Enabled]：システムは、DIMM や CPU などのシステム コンポーネントに対する電力を削減できます。電力削減量は、[Package C State Limit] フィールド**set PackageCStateLimit** コマンドで指定します。
[C1E] ドロップダウン リスト **set ProcessorC1eEnable**	CPU が C1 状態になったときに最低周波数に移行するかどうか。 次のいずれかになります。 • [Disabled]：CPU は C1 状態でも最大周波数で動作し続けます。 • [Enabled]：CPU は最低周波数に移行します。 このオプションを使用すると、C1 状態で電力が最大限に節約されます。 （注） このオプションは、[CPU C State]ProcessorCcxEnable がイネーブルの場合にのみ使用します。

[Memory Configuration] のパラメータ

名前	説明
[Select Memory RAS] ドロップダウン リスト **set SelectMemoryRAS**	サーバのメモリの信頼性、可用性、サービス性（RAS）を設定するかどうか。 次のいずれかになります。 • [Maximum Performance]Maximum_Performance：システムのパフォーマンスが最適化されます。 • [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。 • [Sparing]：一部のメモリが DIMM 障害時の使用のために予約されます。 障害が発生すると、DIMM はオフラインになり、予約済みメモリと交換されます。 このオプションを使用した場合、ミラーリングよりも冗長性が低くなりますが、サーバで実行されているプログラムに使用できるメモリの量は多くなります。

名前	説明
[NUMA Optimized] ドロップダウン リスト **set NUMAOptimize**	BIOS で NUMA をサポートするかどうか。 次のいずれかになります。 • [Disabled]：BIOS で NUMA をサポートしません。 • [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。このオプションをイネーブルにした場合は、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 インターリーブをディセーブルにする必要があります。
[Sparing Mode] ドロップダウン リスト **set SparingMode**	CIMC で使用するスペア モード。 次のいずれかになります。 • [Rank Sparing]Rank_Sparing：スペア メモリはランク レベルで割り当てられます。 • [DIMM Sparing]：スペア メモリは DIMM レベルで割り当てられます。 （注） このオプションは、[Select Memory RAS]set SelectMemoryRAS が [Sparing] に設定されている場合にのみ使用します。
[Mirroring Mode] ドロップダウン リスト **set MirroringMode**	1 つのメモリ ライザーが別のメモリ ライザーとミラーリングされる統合メモリ コントローラ（IMC）間でのミラーリングがサポートされます。 次のいずれかになります。 • [Intersocket]：各 IMC が 2 つのソケット間でミラーリングされます。 • [Intrasocket]：1 つの IMC が同じソケット内の別の IMC とミラーリングされます。 （注） このオプションは、[Select Memory RAS]SelectMemoryRAS が [Mirroring] に設定されている場合にのみ使用します。

名前	説明
[Patrol Scrub] ドロップダウン リスト **set PatrolScrub**	サーバ上のメモリの未使用部分でも、シングル ビット メモリ エラーをシステムでアクティブに検索して修正するかどうか。 次のいずれかになります。 • [Disabled]：CPU によってメモリ アドレスの読み取りまたは書き込みが行われる場合にのみ、システムでメモリの ECC エラーを確認します。 • [Enabled]：システムで定期的にメモリの読み取りおよび書き込みを行って ECC エラーを検索します。 エラーが見つかった場合は修正を試みます。 このオプションによって、シングル ビット エラーをマルチビット エラーになる前に修正できますが、パトロール スクラビング処理の実行時にパフォーマンスが低下する可能性があります。
[Patrol Scrub Interval] ドロップダウン リスト **set PatrolScrubDuration**	パトロール スクラビング処理によるメモリ アクセスの時間間隔を制御します。 間隔が短いほど、メモリのスクラビング処理の頻度が高くなりますが、必要なメモリ帯域幅が多くなります。 5 ～ 23 の範囲の値を選択します。 デフォルト値は、8 です。 （注） このオプションは、[Patrol Scrub] がイネーブルの場合にのみ使用します。
[CKE Low Policy] ドロップダウン リスト **set CKELowPolicy**	DIMM 省電力モード ポリシーを制御します。 次のいずれかになります。 • [Disabled]：DIMM は省電力モードになりません。 • [Slow]：DIMM は省電力モードになる可能性がありますが、要件が高くなります。 したがって、DIMM が省電力モードになる頻度は低くなります。 • [Fast]：DIMM は頻繁に省電力モードになります。 • [Auto]：BIOS は、DIMM の設定に基づいて DIMM が省電力モードになるタイミングを制御します。

[Serial Port Configuration] のパラメータ

名前	説明
[Serial A Enable] ドロップダウン リスト **set Serial-PortA**	シリアル ポート A をイネーブルにするか、ディセーブルにするか。 次のいずれかになります。 • [Disabled]：シリアル ポートはディセーブルになります。 • [Enabled]：シリアル ポートはイネーブルになります。

[USB Configuration] のパラメータ

名前	説明
[Make Device Non-Bootable] ドロップダウン リスト **set MakeUSBDeviceNonBootable**	サーバを USB デバイスからブートできるかどうか。 次のいずれかになります。 • [Disabled]：サーバを USB デバイスからブートできます。 • [Enabled]：サーバを USB デバイスからブートできません。

[PCI Configuration] のパラメータ

名前	説明
[Memory Mapped I/O Above 4GB] ドロップダウン リスト **set MemoryMappedIOAbove4GB**	4 GB 以上のアドレス空間に対する 64 ビット PCI デバイスのメモリ マップ I/O をイネーブルにするか、ディセーブルにするか。 レガシー オプション ROM では、4 GB を超えるアドレスにアクセスできません。 64 ビットに対応し、レガシー オプション ROM を使用する PCI デバイスは、この設定がイネーブルの場合に正しく動作しないことがあります。 次のいずれかになります。 • [Disabled]：サーバは、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プしません。 • [Enabled]：サーバは、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プします。

名前	説明
[Onboard NIC *n* ROM] ドロップダウン リスト **set OnboardNic*n*ROM**	*n* で指定されたオンボード NIC 用に組み込み PXE オプション ROM をシステムでロードするかどうか。 次のいずれかになります。 • [Disabled]：PXE オプション ROM を NIC *n* に使用できません。 • [Enabled]：PXE オプション ROM を NIC *n* に使用できます。
[PCIe OptionROMs] ドロップダウン リスト **set Pci-Opt-Roms**	サーバで PCIe オプション ROM 拡張スロットを使用できるかどうか。 次のいずれかになります。 • [Disabled]：PCIe オプション ROM は使用できません。 • [Enabled]：PCIe オプション ROM を使用できます。
[PCIe Slot *n* ROM] ドロップダウン リスト **set Slot*n*Disable**	*n* で指定された PCIe 拡張スロット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。 • [Disabled]：拡張スロット *n* は使用できません。 • [Enabled]：拡張スロット *n* を使用できます。

C460 サーバのサーバ管理 BIOS パラメータ

名前	説明
[Assert NMI on SERR] ドロップダウン リスト **set AssertNMIOnSERR**	システム エラー（SERR）の発生時に BIOS でマスク不能割り込み（NMI）を生成してエラーをログに記録するかどうか。 次のいずれかになります。 • [Disabled]：SERR の発生時に BIOS で NMI を生成したりエラーをログに記録したりしません。 • [Enabled]：SERR の発生時に BIOS で NMI を生成し、エラーをログに記録します。 [Assert NMI on PERR]Assert_NMI_on_PERR をイネーブルにする場合は、この設定をイネーブルにする必要があります。

名前	説明
[Assert NMI on PERR] ドロップダウン リスト **set AssertNMIOnPERR**	プロセッサ バス パリティ エラー（PERR）の発生時に BIOS でマスク不能割り込み（NMI）を生成してエラーをログに記録するかどうか。 次のいずれかになります。 • [Disabled]：PERR の発生時に BIOS で NMI を生成したりエラーをログに記録したりしません。 • [Enabled]：PERR の発生時に BIOS で NMI を生成し、エラーをログに記録します。 この設定を使用するには、[Assert NMI on SERR]Assert_NMI_on_SERR をイネーブルにする必要があります。
[Console Redirection] ドロップダウン リスト **set ConsoleRedir**	POST 中および BIOS ブート中にコンソール リダイレクションでシリアル ポートを使用できます。 BIOS のブートが終了し、オペレーティング システムがサーバの役割を果たすと、コンソール リダイレクションは無関係になり、効果がなくなります。 次のいずれかになります。 • [Disabled]：POST 中にコンソール リダイレクションは実行されません。 • [Serial Port A]Serial_Port_A：POST 中にシリアル ポート A をコンソール リダイレクション用にイネーブルにします。 （注） このオプションをイネーブルにすると、POST 中に Quiet Boot ロゴ画面の表示がディセーブルになります。
[Flow Control] ドロップダウン リスト **set FlowCtrl**	ハンドシェイク プロトコルをフロー制御に使用するかどうか。 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。 • [None]：フロー制御は使用されません。 • [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 アプリケーションの設定と一致している必要があります。

名前	説明
[Baud Rate] ドロップダウン リスト **set BaudRate**	シリアル ポートの送信速度に使用するボー レート。[Console Redirection] をディセーブルにした場合、このオプションは使用できません。 次のいずれかになります。 • [9.6k]：9600 ボー レートが使用されます。 • [19.2k]：19200 ボー レートが使用されます。 • [38.4k]：38400 ボー レートが使用されます。 • [57.6k]：57600 ボー レートが使用されます。 • [115.2k]：115200 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 アプリケーションの設定と一致している必要があります。
[Terminal Type] ドロップダウン リスト **set TerminalType**	コンソール リダイレクションに使用する文字形式のタイプ。 次のいずれかになります。 • [PC-ANSI]：PC-ANSI 端末フォントが使用されます。 • [VT100]：サポートされている vt100 ビデオ端末とその文字セットが使用されます。 • [VT100-PLUS]：サポートされている vt100-plus ビデオ端末とその文字セットが使用されます。 • [VT-UTF8]：UTF-8 文字セットのビデオ端末が使用されます。 （注） この設定は、リモート ターミナル アプリケーションの設定と一致している必要があります。

名前	説明
[OS Boot Watchdog Timer Timeout] ドロップダウン リスト **set OSBootWatchdogTimerTimeOut**	BIOS でウォッチドッグ タイマーの設定に使用するタイムアウト値。 次のいずれかになります。 • [5 Minutes]5_Minutes：ウォッチドッグ タイマーは、OS のブートが開始されてから 5 分後に期限が切れます。 • [10 Minutes]10_Minutes：ウォッチドッグ タイマーは、OS のブートが開始されてから 10 分後に期限が切れます。 • [15 Minutes]15_Minutes：ウォッチドッグ タイマーは、OS のブートが開始されてから 15 分後に期限が切れます。 • [20 Minutes]20_Minutes：ウォッチドッグ タイマーは、OS のブートが開始されてから 20 分後に期限が切れます。 （注） このオプションは、[OS Boot Watchdog Timer] をイネーブルにした場合にのみ適用されます。
[OS Boot Watchdog Policy] ドロップダウン リスト **set OSBootWatchdogTimerPolicy**	ウォッチドッグ タイマーの期限が切れた場合に実行されるアクション。 次のいずれかになります。 • [Power Off]Power_Off：OS のブート中にウォッチドッグ タイマーの期限が切れた場合、サーバの電源がオフになります。 • [Reset]：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、サーバはリセットされます。 （注） このオプションは、[OS Boot Watchdog Timer] をイネーブルにした場合にのみ適用されます。
[Legacy OS Redirection] ドロップダウン リスト **set LegacyOSRedir**	DOS などのレガシー オペレーティング システムからのリダイレクションをシリアル ポートでイネーブルにするかどうか。 次のいずれかになります。 • [Disabled]：コンソール リダイレクションに対してイネーブルになっているシリアル ポートがレガシー オペレーティング システムで認識されません。 • [Enabled]：コンソール リダイレクションに対してイネーブルになっているシリアル ポートがレガシー オペレーティング システムで認識されます。

名前	説明
[OS Boot Watchdog Timer] ドロップダウン リスト **set OSBootWatchdogTimer**	BIOS で指定されたタイムアウト値を使用してウォッチドッグ タイマーをプログラミングするかどうか。 次のいずれかになります。 • [Disabled]：サーバのブートにかかる時間を追跡するためにウォッチドッグ タイマーは使用されません。 • [Enabled]：サーバのブートにかかる時間を追跡するためにウォッチドッグ タイマーが使用されます。 サーバのブートが指定された時間内に完了しない場合: [OS Boot Watchdog Timer Timeout] フィールドで指定された時間内に完了しない場合は、CIMC によってエラーがログに記録され、[OS Boot Watchdog Policy] フィールドで指定されたアクションが実行されます。**set OSBootWatchdogTimerTimeout** コマンドで指定された時間内に完了しない場合は、CIMC によってエラーがログに記録され、**set OSBootWatchdogTimerPolicy** コマンドで指定されたアクションが実行されます。

索 引

記号

[Navigation] ペイン 5
[Work] ペイン 6

A

Active Directory 62, 63, 64
  設定 64

B

BIOS 152
  TFTP サーバからのインストール 152
  ブラウザ経由のファームウェアのインストール 152
BIOS 設定 20, 32, 33, 35
  高度 33
  サーバ管理 35
  サーバのブート順 20
  主要 32
BIOS パラメータ 169, 170, 183, 186, 187, 198, 201, 202, 213, 217, 218, 229
  C200 および C210 の高度なパラメータ 170
  C200 および C210 のサーバ管理パラメータ 183
  C200 および C210 の主要なパラメータ 169
  C250 の高度なパラメータ 187
  C250 のサーバ管理パラメータ 198
  C250 の主要なパラメータ 186
  C260 の高度なパラメータ 202
  C260 のサーバ管理パラメータ 213
  C260 の主要なパラメータ 201
  C460 の高度なパラメータ 218
  C460 のサーバ管理パラメータ 229
  C460 の主要なパラメータ 217

C

C200 および C210 サーバ 169, 170, 183
  高度な BIOS パラメータ 170
  サーバ管理 BIOS パラメータ 183
  主要な BIOS パラメータ 169
C250 サーバ 186, 187, 198
  高度な BIOS パラメータ 187
  サーバ管理 BIOS パラメータ 198
  主要な BIOS パラメータ 186
C260 サーバ 201, 202, 213
  高度な BIOS パラメータ 202
  サーバ管理 BIOS パラメータ 213
  主要な BIOS パラメータ 201
C460 サーバ 217, 218, 229
  高度な BIOS パラメータ 218
  サーバ管理 BIOS パラメータ 229
  主要な BIOS パラメータ 217
CIMC 147, 148, 149, 150, 151, 155, 156, 157, 158, 163, 165
  出荷時の初期状態へのリセット 165
  ファームウェア 147, 148, 149, 150, 151
    TFTP サーバからのインストール 149
    アクティブ化 151
    概要 147
    シスコからの取得 148
    ブラウザ経由のインストール 150
  リブート 163
  ログしきい値の設定 157
  ログのクリア 156
  ログの送信 158
  ログの表示 155
CIMC GUI 4
CIMC 情報 38
CIMC の概要 2
CPU のプロパティ 39

F

FEX 110
説明 110
プロパティの表示 110
FIP モード 81
Flexible Flash 28, 29, 30, 31
説明 28
ブート 30
プロパティの設定 29
リセット 31

H

HTTP のプロパティ 121

I

IPMI over LAN 124
設定 124
説明 124
IPv4 のプロパティ 72
IP ブロッキング 74

K

KVM 58, 59
イネーブル化 58, 59
設定 58
ディセーブル化 59
KVM コンソール 13, 57
KVM のイネーブル化 58, 59
KVM のディセーブル化 59

L

LED センサー 52

N

NIC プロパティ 70

O

OS のインストール 13, 14, 16
KVM コンソール 14
PXE 16
方法 13

P

PCI アダプタ 43
プロパティの表示 43
PXE のインストール 15

S

Serial over LAN 55
SNMP 126, 127, 128, 129, 142, 143
SNMPv3 ユーザの管理 129
SNMPv3 ユーザの設定 129
テスト メッセージの送信 128, 143
トラップ設定の指定 127, 142
プロパティの設定 126
SSH のプロパティ 122
syslog 158
CIMC ログの送信 158

V

vHBA 83, 88, 92, 93, 94, 95, 96, 97
永続的なバインディング 95
永続的なバインディングのクリア 97
永続的なバインディングの表示 96
管理上の注意事項 83
削除 93
作成 92
ブート テーブル 94
ブート テーブル エントリの削除 95
ブート テーブル エントリの作成 94
プロパティの表示 83
プロパティの変更 88
VLAN のプロパティ 73
VM FEX 110
説明 110
プロパティの表示 110
vNIC 97, 98, 103, 109, 110
管理上の注意事項 97

vNIC *(続き)*
削除 110
作成 109
プロパティの表示 98
プロパティの変更 103

X

XML API 123
説明 123
XML API のプロパティ 123

あ

アダプタ 43, 77, 78, 81, 115, 116, 117, 118, 119
PCI 43
TFTP サーバからのファームウェアのインストール 118
概要 77
構成のインポート 116
構成のエクスポート 115
デフォルト構成の復元 117
ネットワーク 78
ファームウェア 117
ファームウェアのアクティブ化 119
プロパティの設定 81
ローカルファイルからのファームウェアのインストール 117

い

イベント 140
プラットフォーム 140
アラートのイネーブル化 140
アラートのディセーブル化 140
イベント フィルタ、プラットフォーム 139, 140
概要 139
設定 140
イベント ログ、システム 159, 160
クリア 160
表示 159
インポート 167
CIMC 設定 167

え

永続的なバインディング 95, 96, 97
クリア 97
説明 95
表示 96
エクスポート 165, 166
CIMC 設定 165, 166

お

オペレーティング システムのインストール 14
温度センサー 49

か

仮想 KVM 58, 59
仮想メディア 56
仮想メディアの暗号化 56

き

共通プロパティ 72

こ

高度な BIOS パラメータ 170, 187, 202, 218
C200 および C210 サーバ 170
C250 サーバ 187
C260 サーバ 202
C460 サーバ 218
コミュニケーション サービスのプロパティ 121, 122, 123, 124
HTTP のプロパティ 121
IPMI over LAN のプロパティ 124
SSH のプロパティ 122
XML API のプロパティ 123

さ

サーバ概要 1
サーバ管理 17, 19, 20, 22, 23, 24
サーバ電源の再投入 24
サーバのシャットダウン 23

サーバ管理 (続き)
サーバの電源オフ 24
サーバの電源投入 23
サーバのブート順 20
サーバのリセット 22
サーバ ヘルス 17
ロケータ LED 19
サーバ管理 BIOS パラメータ 183, 198, 213, 229
C200 および C210 サーバ 183
C250 サーバ 198
C260 サーバ 213
C460 サーバ 229
サーバ証明書のアップロード 137
サーバ ソフトウェア 2
サーバ電源の再投入 24
サーバの NIC 69
サーバのシャットダウン 23
サーバの電源オフ 24
サーバの電源投入 23
サーバのプロパティ 37
サーバのリセット 22
サーバ ヘルス 17

し

自己署名証明書 135
システム イベント ログ 159, 160
クリア 160
表示 159
主要な BIOS パラメータ 169, 186, 201, 217
C200 および C210 サーバ 169
C250 サーバ 186
C260 サーバ 201
C460 サーバ 217
障害 45
要約の表示 45
障害の要約 45
表示 45
証明書 134
証明書管理 134, 137
新しい証明書 134
証明書のアップロード 137

す

ストレージ センサー 52
ストレージのプロパティ 42
表示 42

せ

設定 165, 166, 167
インポート 167
エクスポート 165
バックアップ 166
センサー 46, 48, 49, 50, 51, 52
LED 52
温度 49
ストレージ 52
電圧 50
電源装置 46
電流 51
ファン 48

つ

ツールバー 9

て

テクニカル サポート データ 161, 162
TFTP へのエクスポート 161
ローカル ファイルへのダウンロード 162
電圧センサー 50
電源センサー 46
電源のプロパティ 42
電流センサー 51
電力制限ポリシー 26
概要 26
設定 26
電力統計情報 25
表示 25
電力復元ポリシー 27
設定 27

ね

ネットワーク アダプタ 78
プロパティの表示 78
ネットワーク セキュリティ 74
ネットワーク プロパティ 70, 72, 73
IPv4 のプロパティ 72
NIC プロパティ 70
VLAN のプロパティ 73
共通プロパティ 72

は

破損した BIOS のリカバリ 164
バックアップ 165, 166
CIMC 設定 165, 166

ふ

ファームウェア 147, 148, 149, 150, 151
TFTP サーバからのインストール 149
アクティブ化 151
概要 147
シスコからの取得 148
ブラウザ経由のインストール 150
ファン センサー 48
ブート順 20, 22
概要 20
設定 20
表示 22
ブート テーブル 94, 95
エントリの削除 95
エントリの作成 94
説明 94
プラットフォーム イベント 140, 143
アラートのイネーブル化 140
アラートのディセーブル化 140
トラップの解釈 143
プラットフォーム イベント フィルタ 139, 140
概要 139
設定 140
フロッピーディスクのエミュレーション 56

め

メモリのプロパティ 39

ゆ

ユーザ管理 61, 64, 66
Active Directory 64
ユーザ セッション 66
ローカル ユーザ 61
ユーザ セッション 66

り

リモート プレゼンス 55, 56, 58, 59
Serial over LAN 55
仮想 KVM 58, 59
仮想メディア 56

ろ

ローカル ユーザ 61
ログアウト 11
ログイン 10
ロケータ LED 19