Cisco UCS C シリーズ サーバ Integrated Management Controller CLI 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 02 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-23490-06-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情報および変更情報 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 CLI 4

コマンド モード 4

コマンド モード表 5

コマンドの実行 8

コマンド履歴 8

保留コマンドのコミット、廃棄、および表示 8

コマンド出力形式 9

CLI に関するオンラインヘルプ 10

サーバ OS のインストール 11

OS のインストール方法 11

KVM コンソール 11

KVM コンソールを使用した OS のインストール 12

PXE インストール サーバ 12

PXE インストール サーバを使用した OS のインストール 13

サーバの管理 15

ロケータ LED の切り替え 15
サーバのブート順の管理 16
サーバのブート順 16
サーバのブート順の設定 16
サーバの実際のブート順の表示 17
サーバのリセット 18
サーバのシャットダウン 19
サーバの電源管理 19
サーバの電源投入 19
サーバの電源オフ 20
サーバ電源の再投入 21
電力ポリシーの設定 21
電力統計情報の表示 21
電力制限ポリシー 23
電力制限ポリシーの設定 23
電力復元ポリシーの設定 24
Flexible Flash コントローラの管理 26
Cisco Flexible Flash 26
Flexible Flash コントローラ プロパティの設定 26
Flexible Flash からのブート 28
Flexible Flash コントローラのリセット 29
BIOS の設定 30
BIOS ステータスの表示 30
主要な BIOS の設定 31
BIOS の詳細設定 32
サーバ管理 BIOS の設定 33
BIOS デフォルトの復元 34
サーバのプロパティの表示 35
サーバのプロパティの表示 35
CIMC のプロパティの表示 36
CPU のプロパティの表示 36
メモリのプロパティの表示 37

電源のプロパティの表示 38
ストレージのプロパティの表示 39
ストレージ アダプタのプロパティの表示 39
Flexible Flash コントローラ プロパティの表示 40
物理ドライブのプロパティの表示 41
仮想ドライブのプロパティの表示 43
PCI アダプタのプロパティの表示 44
ネットワーク関連のプロパティの表示 44
LOM のプロパティの表示 44
サーバのセンサーの表示 47
障害サマリーの表示 47
電源センサーの表示 48
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 50
ストレージ センサーの表示 51
リモート プレゼンスの管理 53
仮想 KVM の管理 53
KVM コンソール 53
仮想 KVM のイネーブル化 54
仮想 KVM のディセーブル化 54
仮想 KVM の設定 55
仮想メディアの設定 56
Serial over LAN の管理 57
Serial Over LAN 57
Serial Over LAN に関するガイドラインおよび制約事項 58
Serial over LAN の設定 58
Serial Over LAN の起動 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 の設定 63
Active Directory 63

Active Directory サーバの設定 63
CIMC での Active Directory の設定 64
CIMC での Active Directory グループの設定 66
ユーザ セッションの表示 68
ユーザ セッションの終了 68
ネットワーク関連の設定 71
サーバ NIC の設定 71
サーバの NIC 71
サーバ NIC の設定 72
共通プロパティの設定 74
IPv4 の設定 74
サーバ VLAN の設定 76
ネットワーク セキュリティの設定 77
ネットワーク セキュリティ 77
ネットワーク セキュリティの設定 77
ネットワーク アダプタの管理 79
Cisco UCS C シリーズ ネットワーク アダプタの概要 79
ネットワーク アダプタのプロパティの表示 80
ネットワーク アダプタのプロパティの設定 81
vHBA の管理 82
vHBA 管理のガイドライン 82
vHBA のプロパティの表示 83
vHBA のプロパティの変更 84
vHBA の作成 89
vHBA の削除 90
vHBA ブート テーブル 91
ブート テーブルの表示 91
ブート テーブル エントリの作成 92
ブート テーブル エントリの削除 93
vHBA の永続的なバインディング 94
永続的なバインディングのイネーブル化 94
永続的なバインディングのディセーブル化 95

永続的なバインディングの再構築 96
vNIC の管理 96
vNIC 管理のガイドライン 96
vNIC のプロパティの表示 97
vNIC のプロパティの変更 98
vNIC の作成 105
vNIC の削除 106
VM FEX の管理 106
仮想マシン ファブリック エクステンダ 106
VM FEX のプロパティの表示 107
VM FEX 設定 109
アダプタ設定のバックアップと復元 113
アダプタ設定のエクスポート 113
アダプタ設定のインポート 114
アダプタのデフォルトの復元 114
アダプタ ファームウェアの管理 115
アダプタ ファームウェア 115
アダプタ ファームウェアのインストール 115
アダプタ ファームウェアのアクティブ化 117
コミュニケーション サービスの設定 119
HTTP の設定 119
SSH の設定 120
XML API の設定 121
CIMC 用の XML API 121
XML API のイネーブル化 121
IPMI の設定 122
IPMI Over LAN 122
IPMI over LAN の設定 122
SNMP の設定 124
SNMP 124
SNMP プロパティの設定 124
SNMP トラップ設定の指定 125
テスト SNMP トラップ メッセージの送信 126

SNMPv3 ユーザの設定 127
証明書の管理 131
サーバ証明書の管理 131
証明書署名要求の生成 132
自己署名証明書の作成 133
サーバ証明書のアップロード 136
プラットフォーム イベント フィルタの設定 137
プラットフォーム イベント フィルタ 137
プラットフォーム イベント アラートのイネーブル化 138
プラットフォーム イベント アラートのディセーブル化 138
プラットフォーム イベント フィルタの設定 139
SNMP トラップ設定の指定 141
テスト SNMP トラップ メッセージの送信 142
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
インストールした CIMC ファームウェアのアクティブ化 150
TFTP サーバからの BIOS ファームウェアのインストール 151
ログの表示 153
CIMC ログ 153
CIMC ログの表示 153
CIMC ログのクリア 154
CIMC ログしきい値の設定 154
リモート サーバへの CIMC ログの送信 156
System Event Log 157
システム イベント ログの表示 157
システム イベント ログのクリア 158
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
CIMC の再起動 162

BIOS CMOS のクリア 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 166
CIMC 設定のエクスポートとインポート 166
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 202
C260 サーバの主要な BIOS パラメータ 202
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 228

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情報および変更情報，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情報および変更情報

次の表は、この最新リリースに関するマニュアルでの主な変更点の概要を示したものです。 ただし、このリリースに関するコンフィギュレーション ガイドの変更点や新機能の中には一部、この表に記載されていないものもあります。 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, （79 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, （79 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, （119 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, （119 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, （119 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 CLI について説明します。
第 2 章	サーバ OS のインストール	サーバ上のオペレーティング システム（OS）の設定方法を説明します。
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を説明します。
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、Active Directory によるユーザ認証の設定方法、ユーザ セッションの管理方法を説明します。
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を説明します。
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 フィルタを設定および管理する方法を説明します。
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 ログとシステム イベント ログのメッセージを表示、エクスポート、およびクリアする方法を説明します。
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
bold 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、**bold** フォントで示しています。
italic 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、*italic* 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}	必ずいずれか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　「時間の節約に役立つ操作」です。 ここに紹介している方法で作業を行うと、時間を短縮できます。

警告　「警告」の意味です。 人身事故を予防するための注意事項が記述されています。

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完全なリストについては、次の URL で入手できる『*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

他のマニュアル リソース

B シリーズと C シリーズのすべてのマニュアルが含まれる 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 ファイルは主要な各マニュアルのリリース後に更新されます。

マニュアルの更新通知を受信するには、Cisco UCS Docs on Twitter 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、または誤りや記載もれなどお気づきの点がございましたら、HTML ドキュメント内のフィードバック フォームよりご連絡ください。 ご協力をよろしくお願いいたします。

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 CLI，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。 専用の ARM ベースのプロセッサが（メイン サーバ CPU から独立して）CIMC ファームウェアを実行します。 システムには、現行バージョンの CIMC ファームウェアが付属しています。 CIMC ファームウェアは更新可能ですが、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ている場合は、UCS Manager を使用してそのサーバを管理する必要があります。 UCS Manager の使用方法については、http://www.cisco.com/go/unifiedcomputing/b-series-doc の『*Cisco UCS B-Series Servers Documentation Roadmap*』にリストされた設定ガイドを参照してください。

管理インターフェイス

Web ベースの GUI または SSH ベースの CLI 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 CLI

CIMC CLI は、Cisco UCS C シリーズ サーバのコマンドライン管理インターフェイスです。 SSH または Telnet を使用し、ネットワークを介して CIMC CLI を起動し、サーバを管理できます。 デフォルトでは、Telnet アクセスはディセーブルになります。

CLI のユーザ ロールは、admin、user（制御は可能、設定は不可）、および read-only のいずれかになります。

（注） admin パスワードが失われたために回復する必要がある場合には、ご使用のプラットフォームの Cisco UCS C シリーズ サーバ インストールおよびサービス ガイドを参照してください。

コマンド モード

CLI のコマンド モードは階層構造になっており、EXEC モードがこの階層の最高レベルとなります。 高いレベルのモードは、低いレベルのモードに分岐します。 **scope** コマンドを使用すると、高いレベルのモードから 1 つ低いレベルのモードに移動し、**exit** コマンドを使用すると、モード階層内の 1 つ高いレベルに移動します。 **top** コマンドを実行すると、EXEC モードに戻ります。

（注） ほとんどのコマンド モードは、管理対象オブジェクトに関連付けられています。 **scope** コマンドを実行すると、管理対象オブジェクトは作成されず、管理対象オブジェクトがすでに存在するモードにアクセスできるだけです。

各モードには、そのモードで入力できるコマンドのセットが含まれています。 各モードで使用できるほとんどのコマンドは、関連付けられた管理対象オブジェクトに関係しています。 割り当てられているロールによっては、あるモードで使用できるコマンドのサブセットにしかアクセスできない場合があります。アクセスできないコマンドは非表示になります。

各モードの CLI プロンプトには、モード階層における現在のモードまでのフルパスが表示されます。 これにより、コマンド モード階層での現在位置がわかりやすくなります。また、階層内を移動する必要がある場合には、非常に便利な機能です。

コマンド モード表

次の表に、最初の 4 レベルのコマンド モード、各モードへのアクセスに使用するコマンド、および各モードに関連付けられている CLI プロンプトを示します。

モード名	アクセスするコマンド	モード プロンプト
EXEC	任意のモードから **top** コマンド	#
bios	EXEC モードから **scope bios** コマンド	/bios #
advanced	BIOS モードから **scope advanced** コマンド	/bios/advanced #
main	BIOS モードから **scope main** コマンド	/bios/main #
server-management	BIOS モードから **scope server-management** コマンド	/bios/server-management #
certificate	EXEC モードから **scope certificate** コマンド	/certificate #
chassis	EXEC モードから **scope chassis** コマンド	/chassis #
adapter	シャーシ モードから **scope adapter** *index* コマンド	/chassis/adapter #
host-eth-if	アダプタ モードから **scope host-eth-if** コマンド	/chassis/adapter/host-eth-if #
host-fc-if	アダプタ モードから **scope host-fc-if** コマンド	/chassis/adapter/host-fc-if #
port-profiles	アダプタ モードから **scope port-profiles** コマンド	/chassis/adapter/port-profiles #
vmfex	アダプタ モードから **scope vmfex** *index* コマンド	/chassis/adapter/vmfex #
dimm-summary	シャーシ モードから **scope dimm-summary** *index* コマンド	/chassis/dimm-summary #
flexflash		/chassis/flexflash #

モード名	アクセスするコマンド	モード プロンプト
	シャーシ モードから **scope flexflash** *index* コマンド	
operational-profiles	flexflash モードから **scope operational-profile** コマンド	/chassis/flexflash/operational-profile #
storageadapter	シャーシ モードから **scope storageadapter** *slot* コマンド	/chassis/storageadapter #
physical-drive	storageadapter モードから **scope physical-drive** コマンド	/chassis/storageadapter/physical-drive #
virtual-drive	storageadapter モードから **scope virtual-drive** コマンド	/chassis/storageadapter/virtual-drive #
cimc	EXEC モードから **scope cimc** コマンド	/cimc #
firmware	cimc モードから **scope firmware** コマンド	/cimc/firmware #
import-export	cimc モードから **scope import-export** コマンド	/cimc/import-export #
log	cimc モードから **scope log** コマンド	/cimc/log #
server	ログ モードから **scope server** *index* コマンド	/cimc/log/server #
network	cimc モードから **scope network** コマンド	/cimc/network #
ipblocking	ネットワーク モードから **scope ipblocking** コマンド	/cimc/network/ipblocking #
tech-support	cimc モードから **scope tech-support** コマンド	/cimc/tech-support #
fault	EXEC モードから **scope fault** コマンド	/fault #
pef	障害モードから **scope pef** コマンド	/fault/pef #

モード名	アクセスするコマンド	モード プロンプト
http	EXEC モードから **scope http** コマンド	/http #
ipmi	EXEC モードから **scope ipmi** コマンド	/ipmi #
kvm	EXEC モードから **scope kvm** コマンド	/kvm #
ldap	EXEC モードから **scope ldap** コマンド	/ldap #
role-group	ldap モードから **scope role-group** コマンド	/ldap/role-group #
power-cap	EXEC モードから **scope power-cap** コマンド	/power-cap #
sel	EXEC モードから **scope sel** コマンド	/sel #
sensor	EXEC モードから **scope sensor** コマンド	/sensor #
snmp	EXEC モードから **scope snmp** コマンド	/snmp #
trap-destination	snmp モードから **scope trap-destination** コマンド	/snmp/trap-destination #
v3users	snmp モードから **scope v3users** コマンド	/snmp/v3users #
sol	EXEC モードから **scope sol** コマンド	/sol #
ssh	EXEC モードから **scope ssh** コマンド	/ssh #
user	EXEC モードから **scope user** *user-number* コマンド	/user #
user-session		/user-session #

モード名	アクセスするコマンド	モード プロンプト
	EXEC モードから **scope user-session** *session-number* コマンド	
vmedia	EXEC モードから **scope vmedia** コマンド	/vmedia #
xmlapi	EXEC モードから **scope xmlapi** コマンド	/xmlapi #

コマンドの実行

任意のモードで Tab キーを使用すると、コマンドを実行できます。 コマンド名の一部を入力して Tab を押すと、コマンド全体が表示されるか、または別のキーワードを選択するか引数値を入力する必要があるところまで表示されます。

コマンド履歴

CLI では、現在のセッションで使用したすべてのコマンドが保存されます。 上矢印キーまたは下矢印キーを使用すると、これまでに使用したコマンドを 1 つずつ表示できます。 上矢印キーを押すと履歴内の直前のコマンドが、下矢印キーを押すと履歴内の次のコマンドが表示されます。 履歴の最後に到達すると、下矢印キーを押しても次のコマンドが表示されなくなります。

履歴内のすべてのコマンドは、履歴を 1 つずつ表示し、目的のコマンドを再度呼び出し、Enter を押すだけでもう一度実行することができます。 このコマンドは手動で入力したように表示されます。 また、コマンドを再度呼び出した後、実行する前にコマンドを変更することもできます。

保留コマンドのコミット、廃棄、および表示

CLI でコンフィギュレーション コマンドを入力する場合、**commit** コマンドを入力するまで、そのコマンドは適用されません。 コミットされるまで、コンフィギュレーション コマンドは保留状態となり、**discard** コマンドを入力して廃棄できます。 保留中のコマンドについては、アスタリスク（*）がコマンド プロンプトの前に表示されます。 この例に示すように、**commit** コマンドを入力するとそのアスタリスクは消えます。

```
Server# scope chassis
Server /chassis # set locator-led off
Server /chassis *# commit
Server /chassis #
```

複数のコマンド モードで保留中の変更を積み重ね、**commit** コマンド 1 つでまとめて適用できます。 任意のコマンド モードで **show configuration pending** コマンドを入力して、保留中のコマンドを表示できます。

（注） 複数のコマンドをまとめてコミットするのは、アトミック操作ではありません。 失敗したコマンドがあっても、成功したコマンドは適用されます。 失敗したコマンドはエラー メッセージで報告されます。

コマンド出力形式

ほとんどの CLI **show** コマンドでは、オプションの **detail** キーワードを指定でき、出力情報は表ではなくリスト形式で表示されます。 **detail** キーワードを使用すると、出力情報を表示するための 2 つの表示形式のいずれかを設定できます。 次の形式を選択できます。

- Default：簡単に確認できるよう、コマンド出力はコンパクト リストで表示されます。

  次に、デフォルト形式のコマンド出力例を示します。

```
Server /chassis # set cli output default
Server /chassis # show hdd detail
Name HDD_01_STATUS:
    Status : present
Name HDD_02_STATUS:
    Status : present
Name HDD_03_STATUS:
    Status : present
Name HDD_04_STATUS:
    Status : present

Server /chassis #
```

- YAML：スクリプトによる解析を簡単に行うため、コマンド出力は、定義された文字列で区切られた YAML（YAML Ain't Markup Language）データ シリアル化言語で表示されます。

  次に、YAML 形式のコマンド出力例を示します。

```
Server /chassis # set cli output yaml
Server /chassis # show hdd detail
---
    name: HDD_01_STATUS
    hdd-status: present

---
    name: HDD_02_STATUS
    hdd-status: present

---
    name: HDD_03_STATUS
    hdd-status: present

---
    name: HDD_04_STATUS
    hdd-status: present

...

Server /chassis #
```

  YAML の詳細については、http://www.yaml.org/about.html を参照してください。

ほとんどの CLI コマンド モードで、**set cli output default** を入力してデフォルト形式を設定するか、**set cli output yaml** を入力して YAML 形式を設定することができます。

CLI に関するオンラインヘルプ

? を入力すれば、いつでも現在のコマンド構文の状態で使用可能なオプションを表示できます。プロンプトに何も入力されていない状態で ? を入力すると、 そのときのモードで使用できるコマンドがすべて表示されます。 コマンドの一部が入力されているときに ? と入力すると、 コマンド構文のそのときの位置で使用できるキーワードと引数がすべて表示されます。

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，11 ページ
- KVM コンソール，11 ページ
- PXE インストール サーバ，12 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） KVM コンソールの操作には、GUI 以外は使用できません。 KVM コンソールの起動手順については、『*Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide*』を参照してください。

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。

- ロケータ LED の切り替え，15 ページ
- サーバのブート順の管理，16 ページ
- サーバのリセット，18 ページ
- サーバのシャットダウン，19 ページ
- サーバの電源管理，19 ページ
- 電力ポリシーの設定，21 ページ
- Flexible Flash コントローラの管理，26 ページ
- BIOS の設定，30 ページ

ロケータ LED の切り替え

はじめる前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **set locator-led** {**on** | **off**}	シャーシ ロケータ LED をイネーブルまたはディセーブルにします。

	コマンドまたはアクション	目的
ステップ 3	Server /chassis # **commit**	トランザクションをシステムの設定にコミットします。

次に、シャーシロケータ LED をディセーブルにして、トランザクションをコミットする例を示します。

```
Server# scope chassis
Server /chassis # set locator-led off
Server /chassis *# commit

Server /chassis #
```

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

（注） ホストが BIOS 電源投入時自己診断テスト（POST）を実行している間は、ブート順を変更しないでください。

はじめる前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope bios**	bios コマンド モードを開始します。
ステップ 2	Server /bios # **set boot-order** *device1*[,*device2*[,*device3*[,*device4*[,*device5*]]]]	ブート デバイス オプションと順序を指定します。次の 1 つ以上を選択できます。 • cdrom：ブート可能な CD-ROM • fdd：フロッピー ディスク ドライブ • hdd：ハード ディスク ドライブ • pxe：PXE ブート • efi：Extensible Firmware Interface
ステップ 3	Server /bios # **commit**	トランザクションをシステムの設定にコミットします。

新規のブート順は、次の BIOS のブートで使用されます。

次に、ブート順を設定し、トランザクションをコミットする例を示します。

```
Server# scope bios
Server /bios # set boot-order hdd,cdrom,fdd,pxe,efi
Server /bios *# commit
Server /bios #  show detail
BIOS:
    Boot Order: HDD,CDROM,FDD,PXE,EFI

Server /bios #
```

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope bios**	bios コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	Server /bios # **show actual-boot-order [detail]**	サーバが最後に起動したときに実際にBIOSで使用されたブート順序を表示します。

次の例では、最後のブートの実際のブート順序を表示します。

```
Server# scope bios
Server /bios #  show actual-boot-order

Boot Order   Type                      Boot Device
------------ ------------------------- ----------------------------------
1            CD/DVD                    CD-ROM
2            CD/DVD                    Cisco   Virtual CD/DVD  1.18
3            Network Device (PXE)      Cisco NIC 23:0.0
4            Network Device (PXE)      MBA v5.0.5  Slot 0100
5            Network Device (PXE)      MBA v5.0.5  Slot 0101
6            Network Device (PXE)      MBA v5.0.5  Slot 0200
7            Network Device (PXE)      MBA v5.0.5  Slot 0201
8            Network Device (PXE)      Cisco NIC 22:0.0
9            Internal EFI Shell        Internal EFI Shell
10           FDD                       Cisco   Virtual HDD     1.18
11           FDD                       Cisco   Virtual Floppy  1.18

Server /bios #
```

サーバのリセット

重要 ファームウェアまたはBIOSの更新が進行中の場合は、そのタスクが完了するまでサーバをリセットしないでください。

はじめる前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシコマンドモードを開始します。
ステップ 2	Server /chassis # **power hard-reset**	確認プロンプトの後に、サーバがリセットされます。

次に、サーバをリセットする例を示します。

```
Server# scope chassis
Server /chassis # power hard-reset
This operation will change the server's power state.
```

```
Continue?[y|N]
```

サーバのシャットダウン

重要 ファームウェアまたは BIOS の更新が進行中の場合は、そのタスクが完了するまでサーバをシャットダウンしないでください。

はじめる前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ モードを開始します。
ステップ 2	Server /chassis # **power shutdown**	サーバをシャットダウンします。

次に、サーバをシャットダウンする例を示します。

```
Server# scope chassis
Server /chassis # power shutdown
```

サーバの電源管理

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。 この場合、CIMC が初期化を完了するまで、サーバはスタンバイ モードに入ります。

重要 ファームウェアまたは BIOS の更新が進行中の場合は、そのタスクが完了するまでサーバの電源を変更しないでください。

はじめる前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **power on**	サーバの電源をオンにします。

次に、サーバの電源をオンにする例を示します。

```
Server# scope chassis
Server /chassis # power on
This operation will change the server's power state.
Continue?[y|N]y

Server /chassis # show
Power Serial Number Product Name  UUID
----- ------------- ------------- ------------------------------------
on    Not Specified Not Specified 208F0100020F000000BEA80000DEAD00
```

サーバの電源オフ

重要 ファームウェアまたは BIOS の更新が進行中の場合は、そのタスクが完了するまでサーバの電源をオフにしないでください。

はじめる前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **power off**	サーバの電源をオフにします。

次に、サーバの電源をオフにする例を示します。

```
Server# scope chassis
Server /chassis # power off
This operation will change the server's power state.
Continue?[y|N]y

Server /chassis # show
Power Serial Number Product Name  UUID
```

```
----- ------------- ------------- ------------------------------------
off   Not Specified Not Specified 208F0100020F000000BEA80000DEAD00
```

サーバ電源の再投入

重要　ファームウェアまたはBIOSの更新が進行中の場合は、そのタスクが完了するまでサーバの電源を再投入しないでください。

はじめる前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope** chassis	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **power cycle**	サーバ電源を再投入します。

次に、サーバ電源を再投入する例を示します。

```
Server# scope chassis
Server /chassis # power cycle
```

電力ポリシーの設定

電力統計情報の表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **show power-cap [detail]**	サーバ電力消費量の統計情報および電力制限ポリシーを表示します。

表示されるフィールドについては、次の表で説明します。

名前	説明
[Current Consumption]	現在サーバによって使用されている電源（ワット単位）。
[Maximum Consumption]	最後にリブートされてからサーバが使用した最大ワット数。
[Minimum Consumption]	最後にリブートされてからサーバが使用した最小ワット数。
[Minimum Configurable Limit]	このサーバのピーク電力キャップとして指定できる最小電力量（ワット単位）。
[Maximum Configurable Limit]	このサーバのピーク電力キャップとして指定できる最大電力量（ワット単位）。

そのほかのフィールドを次の表で説明します。

名前	説明
[Enable Power Capping]	電力キャッピングがイネーブルの場合、システムはサーバに割り当てられる電力量を監視し、サーバがその最大割り当て量を超えると、指定されたアクションを実行します。
[Peak Power]	このサーバに割り当てることのできる最大ワット数。 サーバがこのフィールドに指定されたよりも多くの電力を要求する場合、システムは、[Non-Compliance Action] フィールドに定義されたアクションを実行します。 [Minimum Configurable Limit] フィールドおよび [Maximum Configurable Limit] フィールドに定義された範囲内のワット数を入力します。
[Non-Compliance Action]	電力キャッピングがイネーブルであり、サーバが割り当てられたピーク電力よりも多くを要求する場合に、システムが実行するアクション。 次のいずれかになります。 • **force-power-reduction**：サーバは何らかの方法で強制的に電力消費量を減らします。 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。 • **none**：アクションは実行されず、サーバに対して、[Peak Power] フィールドに指定されたよりも多くの電力の使用が許可されます。 • **power-off-host**：サーバがシャットダウンします。 • **throttle**：サーバで実行中のプロセスのスロットリングが行われ、合計消費電力が抑えられます。

次に、詳細な電力統計情報を表示する例を示します。

```
Server# show power-cap detail
    Cur Consumption (W): 247
    Max Consumption (W): 286
    Min Consumption (W): 229
    Minimum Configurable Limit (W): 285
    Maximum Configurable Limit (W): 1250
    Power Cap Enabled: yes
    Peak Power: 0
    Non Compliance Action: throttle

Server#
```

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、admin 権限を持ってログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope power-cap**	電力制限コマンド モードを開始します。
ステップ 2	Server /power-cap # **set enabled** {**yes** | **no**}	サーバへの電力制限をイネーブルまたはディセーブルにします。
ステップ 3	Server /power-cap # **set peak-power** *watts*	このサーバに割り当てることのできる最大ワット数を指定します。 **show power-cap detail** コマンド出力の [**Minimum Configurable Limit**] フィールドおよび [**Maximum Configurable Limit**] フィールドで定義された範囲内の *watts* 数を入力します。 これらのフィールドは、サーバ モデルによって決まります。

	コマンドまたはアクション	目的
		サーバがこのコマンドで指定されているより多くの電力を要求すると、システムは **set non-compliance-action** コマンドで定義されている処理を実行します。
ステップ 4	Server /power-cap # **set non-compliance-action** {**force-power-reduction** | **none** | **power-off-host** | **throttle**}	電力制限がイネーブルで、ピーク時の電力割り当てよりも大きい電力をサーバで要求している場合にシステムで実行する必要のあるアクションを指定します。 次のいずれかになります。 • **force-power-reduction**：サーバは何らかの方法で強制的に電力消費量を減らします。 このオプションは、一部のサーバ モデルでは使用できません。 • **none**：アクションは実行されず、サーバはピーク時電力設定で指定されているより多くの電力を使用できます。 • **power-off-host**：サーバがシャットダウンされます。 • **throttle**：サーバで実行中のプロセスのスロットリングが行われ、合計消費電力が抑えられます。
ステップ 5	Server /power-cap # **commit**	トランザクションをシステムの設定にコミットします。

次に、電力制限ポリシーをイネーブルにして設定し、トランザクションをコミットする例を示します。

```
Server# scope power-cap
Server /power-cap # set enabled yes
Server /power-cap *# set peak-power 1000
Server /power-cap *# set non-compliance-action throttle
Server /power-cap *# commit
Server /power-cap #  show detail
    Cur Consumption (W): 688
    Max Consumption (W): 1620
    Min Consumption (W): 48
    Minimum Configurable Limit (W): 500
    Maximum Configurable Limit (W): 2000
    Power Cap Enabled: yes
    Peak Power: 1000
    Non Compliance Action: throttle

Server /power-cap #
```

電力復元ポリシーの設定

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

はじめる前に

このタスクを実行するには、admin 権限を持ってログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **set policy** {**power-off** | **power-on** | **restore-last-state**}	シャーシの電源が復旧した場合に実行するアクションを指定します。 次のいずれかを選択します。 • **power-off**：サーバの電源は、手動で投入されるまでオフのままになります。 これがデフォルトのアクションになります。 • **power-on**：シャーシの電源が回復したときにサーバの電源がオンになります。 • **restore-last-state**：サーバの電源は、シャーシの電源が切断される前の状態に戻ります。 選択したアクションが **power-on** の場合は、サーバに対して電源を回復するまでの遅延を選択できます。
ステップ 3	Server /chassis # **set delay** {**fixed** | **random**}	（任意） サーバの電源復元までの時間を固定するか、ランダムにするかを指定します。デフォルトは**fixed**です。 このコマンドは、電力復元アクションが **power-on** の場合のみ使用可能です。
ステップ 4	Server /chassis # **set delay-value** *delay*	（任意） 遅延時間を秒単位で指定します。 指定できる範囲は 0 ～ 240 です。デフォルト値は 0 です。
ステップ 5	Server /chassis # **commit**	トランザクションをシステムの設定にコミットします。

次に、180秒（3分）の固定遅延で電源をオンにする電力復元ポリシーを設定し、トランザクションをコミットする例を示します。

```
Server# scope chassis
Server /chassis # set policy power-on
Server /chassis *# set delay fixed
Server /chassis *# set delay-value 180
Server /chassis *# commit
Server /chassis #  show detail
Chassis:
    Power: on
    Serial Number: QCI1404A1IT
    Product Name: UCS C200 M1
```

```
    PID : R200-1120402
    UUID: 01A6E738-D8FE-DE11-76AE-8843E138AE04
    Locator LED: off
    Description: Testing power restore
    Power Restore Policy: power-on
    Power Delay Type: fixed
    Power Delay Value(sec): 180

Server /chassis #
```

Flexible Flash コントローラの管理

Cisco Flexible Flash

C シリーズ ラックマウント サーバ の中には、サーバ ソフトウェア ツールおよびユーティリティのストレージとして、内蔵 Secure Digital（SD）メモリ カードをサポートしているものがあります。 この SD カードは Cisco Flexible Flash ストレージ アダプタでホストされます。

CIMC は、SD ストレージを 4 つの仮想 USB ドライブとして使用できます。 4 つの仮想 USB ドライブのうち3つはシスコ ソフトウェアにあらかじめロードされており、4つ目はユーザがハイパーバイザまたはその他のコンテンツにインストールします。 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）
- ユーザがインストール（ブート可能な場合あり）
- シスコ ドライバ（ブート不可）
- Cisco Host Upgrade Utility（ブート可能）

シスコ ソフトウェア ユーティリティおよびパッケージの詳細については、次の URL の『*Cisco UCS C-Series Servers Documentation Roadmap*』を参照してください。

http://www.cisco.com/go/unifiedcomputing/c-series-doc

Flexible Flash コントローラ 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 権限を持ってログインする必要があります。
- お使いのプラットフォームで Cisco Flexible Flash がサポートされている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	Server /chassis # **scope flexflash** *index*	指定コントローラに対して Cisco Flexible Flash コントローラ コマンド モードを開始します。 この時点では、許容される *index* 値は **FlexFlash-0** だけです。
ステップ 3	Server /chassis/flexflash # **scope operational-profile**	Operational Profile コマンド モードを開始します。
ステップ 4	Server /chassis/flexflash/operational-profile # **set error-count-threshold**	Cisco Flexible Flash カードへのアクセス中に許可される読み取り/書き込みエラーの数を指定します。 エラー数がこのしきい値を超えると、Cisco Flexible Flash カードがディセーブルになります。CIMC が再アクセスを試みる前に、カードをリセットする必要があります。 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。 検出されたエラー数に関係なく、カードがディセーブルにならないように指定するには、0（ゼロ）を入力します。
ステップ 5	Server /chassis/flexflash/operational-profile # **set raid-primary-member** {**slot1** | **slot2**}	データのプライマリ コピーが存在するスロット。 **重要** 現在、Cisco Flexible Flash カードはスロット 1 でのみサポートされています。 したがって、このフィールドは **slot1** に設定する必要があります。
ステップ 6	Server /chassis/flexflash/operational-profile # **set virtual-drives-enabled** *list*	サーバから USB 形式のドライブとして使用できるようにする仮想ドライブのリストを指定します。 オプションは次のとおりです。 • SCU：サーバは Cisco UCS-Server Configuration Utility にアクセスできます。 • DRIVERS：サーバはシスコ ドライバ ボリューム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。 複数のオプションを指定する場合は、リストを引用符（"）で囲む必要があります。
ステップ 7	Server /chassis/adapter # **commit**	トランザクションをシステムの設定にコミットします。

この例では、フラッシュ コントローラのプロパティを設定します。

```
Server# scope chassis
Server /chassis # scope flexflash FlexFlash-0
Server /chassis/flexflash # scope operational-profile
Server /chassis/flexflash/operational-profile # set error-count-threshold 100
Server /chassis/flexflash/operational-profile *# set raid-primary-member slot1
Server /chassis/flexflash/operational-profile *# set virtual-drives-enabled "SCU HUU"
Server /chassis/flexflash/operational-profile *# commit
Server /chassis/flexflash/operational-profile #
```

Flexible Flash からのブート

Cisco Flexible Flash カード上のブート可能な仮想ドライブを指定して、サーバが次に再起動されたときにそのドライブをデフォルトのブートプライオリティよりも優先させることができます（サーバに定義されているデフォルト ブート順は無視されます）。 指定したブート デバイスは一度だけ使用されます。 サーバがリブートした後、この設定は無効になります。

（注） サーバをリブートする前に、選択する仮想ドライブが Cisco Flexible Flash カード上でイネーブルになっていることを確認してください。

はじめる前に

- このタスクを実行するには、admin 権限を持ってログインする必要があります。
- お使いのプラットフォームで Cisco Flexible Flash がサポートされている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope bios**	BIOS コマンド モードを開始します。
ステップ 2	Server /bios # **set boot-override** {**None** | **SCU** | **HV** | **HUU**}	次回サーバが再起動されるときにブートを試行する仮想ドライブ。 次のいずれかになります。 • None：サーバはデフォルトのブート オーダーを使用します • SCU：サーバは Cisco UCS-Server Configuration Utility からブートします • HV：サーバはハイパーバイザ仮想ドライブから起動します • HUU：サーバは Cisco Host Upgrade Utility からブートします

	コマンドまたはアクション	目的
ステップ 3	Server /bios # **commit**	トランザクションをシステムの設定にコミットします。

この例では、サーバが次の再起動時に Cisco UCS-Server Configuration Utility からブートするよう指定します。

```
Server# scope bios
Server /bios # set boot-override SCU
Committing the boot override BIOS will try boot to
the specified boot device first. Failure to detect
the boot device BIOS will boot from the list
configured in the BIOS boot order.
Server /bios *# commit
Server /bios #
```

Flexible Flash コントローラのリセット

通常の操作では、Cisco Flexible Flash のリセットが必要になることはありません。 テクニカル サポートの担当者から明確に指示された場合にだけ、この手順を実行することを推奨します。

（注） この操作は、Cisco Flexible Flash コントローラ上の仮想ドライブへのトラフィックを中断させます。

はじめる前に

- このタスクを実行するには、admin 権限を持ってログインする必要があります。
- お使いのプラットフォームで Cisco Flexible Flash がサポートされている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scope flexflash** *index*	指定コントローラに対して Cisco Flexible Flash コントローラ コマンド モードを開始します。この時点では、許容される *index* 値は **FlexFlash-0** だけです。
ステップ 3	Server /chassis/flexflash # **reset**	Cisco Flexible Flash コントローラをリセットします。

この例では、フラッシュ コントローラをリセットします。

```
Server# scope chassis
Server /chassis # scope flexflash FlexFlash-0
Server /chassis/flexflash # reset
This operation will reset Cisco Flexible Flash controller.
Host traffic to VDs on this device will be disrupted.
Continue?[y|N] y

Server /chassis/flexflash #
```

BIOS の設定

BIOS ステータスの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope bios**	BIOS コマンド モードを開始します。
ステップ 2	Server /bios # **show detail**	BIOS ステータスの詳細を表示します。

BIOS ステータス情報には、次のフィールドが含まれます。

名前	説明
BIOS Version	実行中の BIOS のバージョン文字列。
Boot Order	サーバが使用を試行する、ブート可能なターゲット タイプの順序。
Boot Override Priority	None、SCU、HV、HUU のいずれかになります。
FW Update/Recovery Status	保留中のファームウェア アップデートまたは回復アクションのステータス。
FW Update/Recovery Progress	直近のファームウェア アップデートまたは回復アクションの完了率。

次に、BIOS ステータスを表示する例を示します。

```
Server# scope bios
Server /bios # show detail
    BIOS Version: "C460M1.1.2.2a.0 (Build Date: 01/12/2011)"
    Boot Order: EFI,CDROM,HDD
    Boot Override Priority:
```

```
    FW Update/Recovery Status: NONE
    FW Update/Recovery Progress: 100

Server /bios #
```

主要な BIOS の設定

はじめる前に

このタスクを実行するには、admin 権限を持ってログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope bios**	BIOS コマンド モードを開始します。
ステップ 2	Server /bios # **scope main**	主要な BIOS 設定コマンド モードを開始します。
ステップ 3	BIOS 設定を設定します。	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 , （202 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 4	Server /bios/main # **commit**	トランザクションをシステムの設定にコミットします。 変更はサーバの次のリブート時に適用されます。 サーバの電源がオンの場合、ただちに再起動するかどうかを選択するように求められます。

この例では、重大な POST エラーの発生時にブートを一時停止するよう BIOS を設定し、トランザクションをコミットします。

```
Server# scope bios
Server /bios # scope main
Server /bios/main # set POSTErrorPause Enabled
Server /bios/main *# commit
```

```
Changes to BIOS set-up parameters will require a reboot.
Do you want to reboot the system?[y|N] n
Changes will be applied on next reboot.
Server /bios/main #
```

BIOS の詳細設定

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

はじめる前に

このタスクを実行するには、admin 権限を持ってログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope bios**	BIOS コマンド モードを開始します。
ステップ 2	Server /bios # **scope advanced**	高度な BIOS 設定コマンド モードを開始します。
ステップ 3	BIOS 設定を設定します。	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 4	Server /bios/advanced # **commit**	トランザクションをシステムの設定にコミットします。 変更はサーバの次のリブート時に適用されます。 サーバの電源がオンの場合、ただちに再起動するかどうかを選択するように求められます。

この例では、低電圧 DDR メモリ モードを有効にし、トランザクションをコミットします。

```
Server# scope bios
Server /bios # scope advanced
Server /bios/advanced # set LvDDRMode Enabled
Server /bios/advanced *# commit
Changes to BIOS set-up parameters will require a reboot.
Do you want to reboot the system?[y|N] n
Changes will be applied on next reboot.
Server /bios/advanced #
```

サーバ管理 BIOS の設定

はじめる前に

このタスクを実行するには、admin 権限を持ってログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope bios**	BIOS コマンド モードを開始します。
ステップ 2	Server /bios # **scope server-management**	サーバ管理 BIOS 設定コマンド モードを開始します。
ステップ 3	BIOS 設定を設定します。	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，（228 ページ）
ステップ 4	Server /bios/server-management # **commit**	トランザクションをシステムの設定にコミットします。 変更はサーバの次のリブート時に適用されます。 サーバの電源がオンの場合、ただちに再起動するかどうかを選択するように求められます。

この例では、BMC の自動検出をイネーブルにし、トランザクションをコミットします。

```
Server# scope bios
Server /bios # scope server-management
Server /bios/server-management # set BMCPnP Enabled
Server /bios/server-management *# commit
Changes to BIOS set-up parameters will require a reboot.
Do you want to reboot the system?[y|N] n
Changes will be applied on next reboot.
Server /bios/server-management #
```

BIOS デフォルトの復元

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope bios**	BIOS コマンド モードを開始します。
ステップ 2	Server /bios # **bios-setup-default**	BIOS のデフォルト設定を復元します。 このコマンドでは、リブートが開始されます。

次の例は、BIOS デフォルト設定を復元します。

```
Server# scope bios
Server /bios # bios-setup-default
This operation will reset the BIOS set-up tokens to factory defaults.
All your configuration will be lost.
Changes to BIOS set-up parameters will initiate a reboot.
Continue?[y|N]y
```

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，35 ページ
- CIMC のプロパティの表示，36 ページ
- CPU のプロパティの表示，36 ページ
- メモリのプロパティの表示，37 ページ
- 電源のプロパティの表示，38 ページ
- ストレージのプロパティの表示，39 ページ
- PCI アダプタのプロパティの表示，44 ページ
- ネットワーク関連のプロパティの表示，44 ページ

サーバのプロパティの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **show chassis** [**detail**]	サーバのプロパティを表示します。

次に、サーバのプロパティを表示する例を示します。

```
Server# show chassis detail
Chassis:
    Power: on
    Serial Number: QCI140205ZG
    Product Name: UCS C210 M2
    PID : R210-2121605W
    UUID: FFFFFFFF-FFFF-FFFF-FFFF-FFFFFFFFFFFF
    Locator LED: off
```

```
    Description:
    Power Restore Policy: power-off
    Power Delay Type: fixed
    Power Delay Value(sec): 0

Server#
```

CIMC のプロパティの表示

（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。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **show cimc** [**detail**]	CIMC のプロパティを表示します。

次に、CIMC のプロパティを表示する例を示します。

```
Server# show cimc detail
CIMC:
    Firmware Version: 1.4(2.18)
    Current Time: Wed Jan 11 07:01:50 2012
    Boot-loader Version: 1.4(2.18).16

Server#
```

CPU 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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **show cpu** [**detail**]	CPU のプロパティを表示します。

次に、CPU のプロパティを表示する例を示します。

```
Server# scope chassis
Server /chassis # show cpu
Name         Cores    Version
------------ -------- ----------------------------------------------------
CPU1         4        Intel(R) Xeon(R) CPU           E5520  @ 2.27GHz
CPU2         4        Intel(R) Xeon(R) CPU           E5520  @ 2.27GHz

Server /chassis #
```

メモリ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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **show dimm** [**detail**]	メモリのプロパティを表示します。
ステップ 3	Server /chassis # **show dimm-summary**	DIMM サマリー情報を表示します。

次に、メモリのプロパティを表示する例を示します。

```
Server# scope chassis
Server /chassis # show dimm
Name                 Capacity        Channel Speed (MHz) Channel Type
-------------------- --------------- ------------------- ---------------
DIMM_A1              2048 MB         1067                Other
DIMM_A2              2048 MB         1067                Other
DIMM_B1              2048 MB         1067                Other
DIMM_B2              2048 MB         1067                Other
DIMM_C1              Not Installed   Unknown             Other
DIMM_C2              Not Installed   Unknown             Other
DIMM_D1              2048 MB         1067                Other
DIMM_D2              2048 MB         1067                Other
DIMM_E1              2048 MB         1067                Other
DIMM_E2              2048 MB         1067                Other
DIMM_F1              Not Installed   Unknown             Other
DIMM_F2              Not Installed   Unknown             Other

Server /chassis #
```

次に、メモリのプロパティに関する詳細情報を表示する例を示します。

```
Server# scope chassis
Server /chassis # show dimm detail
Name DIMM_A1:
    Capacity: 2048 MB
    Channel Speed (MHz): 1067
    Channel Type: Other
    Memory Type Detail: Synchronous
    Bank Locator: NODE 0 CHANNEL 0 DIMM 0
    Visibility: Yes
```

```
    Operability: Operable
    Manufacturer: 0x802C
    Part Number: 18JSF25672PY-1G1D1
    Serial Number: 0xDA415F3F
    Asset Tag: Unknown
    Data Width: 64 bits
Name DIMM_A2:
    Capacity: 2048 MB
--More--

Server /chassis #
```

次の例では、DIMM サマリー情報を表示します。

```
Server# scope chassis
Server /chassis # show dimm-summary
DIMM Summary:
    Memory Speed: 1067 MHz
    Total Memory: 16384 MB
    Effective Memory: 16384 MB
    Redundant Memory: 0 MB
    Failed Memory: 0 MB
    Ignored Memory: 0 MB
    Number of Ignored Dimms: 0
    Number of Failed Dimms: 0
    Memory RAS possible: Memory configuration can support mirroring
    Memory Configuration: Maximum Performance

Server /chassis #
```

電源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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **show psu** [**detail**]	電源のプロパティを表示します。

次に、電源のプロパティを表示する例を示します。

```
Server# scope chassis
Server /chassis # show psu
Name       In. Power (Watts)    Out. Power (Watts)   Firmware  Status
---------- -------------------- -------------------- -------- ----------
PSU1       74                   650                  R0E      Present
PSU2       83                   650                  R0E      Present

Server /chassis #
```

ストレージのプロパティの表示

ストレージ アダプタのプロパティの表示

はじめる前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **show storageadapter** [*slot*] [**detail**]	インストールされているストレージカードを表示します。 （注） このコマンドは、CIMC経由で管理できるサーバの MegaRAID のすべてのコントローラを表示します。インストールされているコントローラまたはストレージ デバイスが表示されない場合、CIMC経由で管理できません。
ステップ 3	Server /chassis # **scope storageadapter** *slot*	装着されているストレージカードに対してコマンド モードを開始します。
ステップ 4	Server /chassis/storageadapter # **show bbu** [**detail**]	ストレージ カードのバッテリ バックアップ ユニットの情報を表示します。
ステップ 5	Server /chassis/storageadapter # **show capabilites** [**detail**]	ストレージカードでサポートされる RAID レベルを表示します。
ステップ 6	Server /chassis/storageadapter # **show error-counters** [**detail**]	ストレージカードによって認識されたエラーの数を表示します。
ステップ 7	Server /chassis/storageadapter # **show firmware-versions** [**detail**]	ストレージカードのファームウェア バージョン情報を表示します。
ステップ 8	Server /chassis/storageadapter # **show hw-config** [**detail**]	ストレージカードのハードウェア情報を表示します。
ステップ 9	Server /chassis/storageadapter # **show mfg-data** [**detail**]	ストレージカードの製造元のデータを表示します。

	コマンドまたはアクション	目的
ステップ 10	Server /chassis/storageadapter # **show pci-info** [**detail**]	ストレージ カードのディスプレイ アダプタの PCI 情報が表示されます。
ステップ 11	Server /chassis/storageadapter # **show running-firmware-images** [**detail**]	ストレージカードの実行中のファームウェアの情報を表示します。
ステップ 12	Server /chassis/storageadapter # **show settings** [**detail**]	ストレージ カードのアダプタ ファームウェアの設定を表示します。
ステップ 13	Server /chassis/storageadapter # **show startup-firmware-images** [**detail**]	ストレージカードの起動時にアクティブにするファームウェア イメージを表示します。

次に、ストレージのプロパティを表示する例を示します。

```
Server# scope chassis
Server /chassis # show storageadapter
PCI Slot Product Name                       Serial Number  Firmware Package Build
-------- ---------------------------------- -------------- -------------------------
SAS      LSI MegaRAID SAS 9260-8i           SV93404392     12.12.0-0038


         Product ID     Battery Status Cache Memory Size
     ---- -------------- -------------- --------------
         LSI Logic      fully charged  0 MB

Server /chassis #
```

この例では、SAS という名前のストレージ カードのバッテリ バックアップ ユニットの情報を表示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SAS
Server /chassis/storageadapter # show bbu
Controller Battery Type Battery Present Voltage    Current    Charge Charging State
---------- ------------ --------------- ---------- ---------- ------ --------------
SAS        iBBU         true            4.051 V    0.000 A    100%   fully charged

Server /chassis/storageadapter #
```

Flexible Flash コントローラ プロパティの表示

はじめる前に

- お使いのプラットフォームで Cisco Flexible Flash がサポートされている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	Server /chassis # **show flexflash [detail]**	（任意）使用可能な Cisco Flexible Flash コントローラを表示します。
ステップ 3	Server /chassis # **scope flexflash** *index*	指定コントローラに対して Cisco Flexible Flash コントローラ コマンドモードを開始します。この時点では、許容される *index* 値は **FlexFlash-0** だけです。
ステップ 4	Server /chassis/flexflash # **show operational-profile [detail]**	Operational Profile のプロパティを表示します。

この例では、フラッシュ コントローラのプロパティを表示します。

```
Server# scope chassis
Server /chassis # show flexflash
Controller   Product Name     Has Error  Firmware Version  Vendor   Internal State
------------ ---------------- ---------- ----------------- -------- ---------------
FlexFlash-0  Cisco FlexFlash  No         1.2 build 247     Cypress  Connected

Server /chassis # scope flexflash FlexFlash-0
Server /chassis # show operational-profile
Primary Member Slot  I/O Error Threshold  Host Accessible VDs
-------------------- -------------------- --------------------
slot1                100                   SCU Drivers

Server /chassis/flexflash #
```

物理ドライブのプロパティの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンドモードを開始します。
ステップ 2	Server /chassis # **scope storageadapter** *slot*	装着されているストレージ カードに対してコマンド モードを開始します。
ステップ 3	Server /chassis/storageadapter # **show physical-drive** [*drive-number*] [**detail**]	ストレージ カードの物理ドライブの情報を表示します。
ステップ 4	Server /chassis/storageadapter # **show physical-drive-count** [**detail**]	ストレージ カードの物理ドライブの数を表示します。
ステップ 5	Server /chassis/storageadapter # **scope physical-drive** *drive-number*	指定された物理ドライブのコマンドモードを開始します。

	コマンドまたはアクション	目的
ステップ 6	Server /chassis/storageadapter/physical-drive # **show general** [**detail**]	指定された物理ドライブに関する一般情報を表示します。
ステップ 7	Server /chassis/storageadapter/physical-drive # **show inquiry-data** [**detail**]	指定された物理ドライブに関する問い合わせのデータを表示します。
ステップ 8	Server /chassis/storageadapter/physical-drive # **show status** [**detail**]	指定された物理ドライブのステータス情報を表示します。

この例では、SAS という名前のストレージ カードの物理ドライブ番号 1 に関する一般情報を表示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SAS
Server /chassis/storageadapter # scope physical-drive 1
Server /chassis/storageadapter/physical-drive # show general
Slot Number 1:
    Controller: SAS
    Enclosure Device ID: 27
    Device ID: 34
    Sequence Number: 2
    Media Error Count: 0
    Other Error Count: 0
    Predictive Failure Count: 0
    Link Speed: 6.0 Gb/s
    Interface Type: SAS
    Media Type: HDD
    Block Size: 512
    Block Count: 585937500
    Raw Size: 286102 MB
    Non Coerced Size: 285590 MB
    Coerced Size: 285568 MB
    SAS Address 0: 500000e112693fa2
    SAS Address 1:
    Connected Port 0:
    Connected Port 1:
    Connected Port 2:
    Connected Port 3:
    Connected Port 4:
    Connected Port 5:
    Connected Port 6:
    Connected Port 7:
    Power State: powersave

Server /chassis/storageadapter/physical-drive #
```

この例では、SAS という名前のストレージ カードの物理ドライブ番号 1 に関する問い合わせデータを表示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SAS
Server /chassis/storageadapter # scope physical-drive 1
Server /chassis/storageadapter/physical-drive # show inquiry-data
Slot Number 1:
    Controller: SAS
    Product ID: MBD2300RC
    Drive Firmware: 5701
    Drive Serial Number: D010P9A0016D
```

```
Server /chassis/storageadapter/physical-drive #
```

この例では、SAS という名前のストレージ カードの物理ドライブ番号 1 のステータス情報を表示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SAS
Server /chassis/storageadapter # scope physical-drive 1
Server /chassis/storageadapter/physical-drive # show inquiry-data
Slot Number 1:
    Controller: SAS
    State: online
    Online: true
    Fault: false

Server /chassis/storageadapter/physical-drive #
```

仮想ドライブのプロパティの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scope storageadapter** *slot*	装着されているストレージ カードに対してコマンド モードを開始します。
ステップ 3	Server /chassis/storageadapter # **show virtual-drive** [*drive-number*] [**detail**]	ストレージ カードの仮想ドライブの情報を表示します。
ステップ 4	Server /chassis/storageadapter # **show virtual-drive-count** [**detail**]	ストレージ カードに設定された仮想ドライブの数を表示します。
ステップ 5	Server /chassis/storageadapter # **scope virtual-drive** *drive-number*	指定された仮想ドライブのコマンド モードを開始します。
ステップ 6	Server /chassis/storageadapter/virtual-drive # **show physical-drive** [**detail**]	指定した仮想ドライブに関する物理ドライブ情報を表示します。

この例では、SAS という名前のストレージ カードの仮想ドライブに関する情報を表示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SAS
Server /chassis/storageadapter # show virtual-drive
Virtual Drive  Status          Name                     Size       RAID Level
-------------- --------------- ------------------------ ---------- ----------
0              Optimal         SLES1SP1beta5            30720 MB   RAID 0
1              Optimal         RHEL5.5                  30720 MB   RAID 0
2              Optimal         W2K8R2_DC                30720 MB   RAID 0
3              Optimal         VD_3                     30720 MB   RAID 0
4              Optimal         ESX4.0u2                 30720 MB   RAID 0
5              Optimal         VMs                      285568 MB  RAID 0
6              Optimal         RHEL6-35GB               35840 MB   RAID 0
7              Optimal         OS_Ins_Test_DR           158720 MB  RAID 0
```

```
8             Optimal                                 285568 MB  RAID 1

Server /chassis/storageadapter #
```

この例では、SAS という名前のストレージ カード上の仮想ドライブ番号 1 に関する物理ドライブ情報を表示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SAS
Server /chassis/storageadapter # scope virtual-drive 1
Server /chassis/storageadapter/virtual-drive # show physical-drive
Span  Physical Drive Status     Starting Block Number Of Blocks
----- -------------- ---------- -------------- ----------------
0     12             online     62914560       62914560

Server /chassis/storageadapter/virtual-drive #
```

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **show pci-adapter** [**detail**]	PCI アダプタのプロパティを表示します。

次に、PCI アダプタのプロパティを表示する例を示します。

```
Server# scope chassis
Server /chassis # show pci-adapter
Name              Slot  Vendor ID    Device ID    Product Name
----------------- ----- ------------ ------------ -------------------------
PCIe Adapter1     1     0x1137       0x0042       Cisco UCS P81E Virtual...
PCIe Adapter2     5     0x1077       0x2432       Qlogic QLE2462 4Gb dua...

Server /chassis #
```

ネットワーク関連のプロパティの表示

LOM のプロパティの表示

LAN On Motherboard（LOM）イーサネット ポートの MAC アドレスを表示できます。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope network**	ネットワーク コマンド モードを開始します。
ステップ 3	Server /cimc/network # **show lom-mac-list** [**detail**]	LOM ポートの MAC アドレスを表示します。

次に、LOM ポートの MAC アドレスを表示する例を示します。

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # show lom-mac-list
Interface       MAC Address
--------------- --------------------
eth0            010000002000
eth1            010000002000

Server /cimc/network #
```

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。

- 障害サマリーの表示，47 ページ
- 電源センサーの表示，48 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，50 ページ
- ストレージ センサーの表示，51 ページ

障害サマリーの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope fault**	障害コマンド モードを開始します。
ステップ 2	Server /fault # **show discrete-alarm [detail]**	個別センサーからの障害の概要が表示されます。
ステップ 3	Server /fault # **show threshold-alarm [detail]**	しきい値センサーからの障害の概要が表示されます。

次の例では、個別センサーからの障害の概要が表示されます。

```
Server# scope fault
Server /fault # show discrete-alarm
```

```
Name         Reading              Sensor Status
------------ -------------------- ------------------------------------
PSU2_STATUS  absent               Critical

Server /fault #
```

電源センサーの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope sensor**	センサー コマンド モードを開始します。
ステップ 2	Server /sensor # **show psu** [**detail**]	サーバの電源センサーの統計情報を表示します。
ステップ 3	Server /sensor # **show psu-redundancy** [**detail**]	サーバの電源冗長センサーのステータスを表示します。

次に、電源センサーの統計情報を表示する例を示します。

```
Server# scope sensor
Server /sensor # show psu
Name                Sensor Status        Reading    Units      Min. Warning    Max. Warning
    Min. Failure    Max. Failure
------------------- -------------------- ---------- ---------- --------------
--------------- --------------- ---------------
PSU1_STATUS          Normal               present

PSU2_STATUS          Normal               present

Server /sensor # show psu-redundancy
Name                Reading    Sensor Status
------------------- ---------- --------------------
PSU_REDUNDANCY       full       Normal

Server /sensor #
```

ファン センサーの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope sensor**	センサー コマンド モードを開始します。
ステップ 2	Server /sensor # **show fan** [**detail**]	サーバのファンセンサーの統計情報を表示します。

次に、ファン センサーの統計情報を表示する例を示します。

```
Server# scope sensor
Server /sensor # show fan
Name                  Sensor Status  Reading    Units      Min. Warning    Max. Warning
Min. Failure    Max. Failure
--------------------- -------------- ---------- ---------- --------------- ---------------
--------------- ---------------
W793_FAN2_TACH1       Normal         2400       RPM        N/A             N/A
800             N/A
W793_FAN2_TACH2       Normal         2400       RPM        N/A             N/A
800             N/A
W793_FAN3_TACH1       Normal         2300       RPM        N/A             N/A
800             N/A
W793_FAN3_TACH2       Normal         2300       RPM        N/A             N/A
800             N/A
W793_FAN4_TACH1       Normal         2400       RPM        N/A             N/A
800             N/A
W793_FAN4_TACH2       Normal         1600       RPM        N/A             N/A
800             N/A

Server /sensor #
```

温度センサーの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope sensor**	センサー コマンド モードを開始します。
ステップ 2	Server /sensor # **show temperature** [**detail**]	サーバの温度センサーの統計情報を表示します。

次に、温度センサーの統計情報を表示する例を示します。

```
Server# scope sensor
Server /sensor # show temperature
Name                        Sensor Status  Reading    Units      Min. Warning Max. Warning
Min. Failure Max. Failure
--------------------------- -------------- ---------- ---------- ------------ ------------
------------ ------------
IOH_TEMP_SENS               Normal         32.0       C          N/A          80.0
N/A          85.0
P2_TEMP_SENS                Normal         31.0       C          N/A          80.0
N/A          81.0
P1_TEMP_SENS                Normal         34.0       C          N/A          80.0
N/A          81.0
DDR3_P2_D1_TMP              Normal         20.0       C          N/A          90.0
N/A          95.0
DDR3_P1_A1_TMP              Normal         21.0       C          N/A          90.0
N/A          95.0
FP_AMBIENT_TEMP             Normal         28.0       C          N/A          40.0
N/A          45.0

Server /sensor #
```

電圧センサーの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope sensor**	センサー コマンドモードを開始します。
ステップ 2	Server /sensor # **show voltage** [**detail**]	サーバの電圧センサーの統計情報を表示します。

次に、電圧センサーの統計情報を表示する例を示します。

```
Server# scope sensor
Server /sensor # show voltage
Name                     Sensor Status  Reading    Units      Min. Warning Max. Warning
Min. Failure Max. Failure
------------------------ -------------- ---------- ---------- ------------ ------------
------------ ------------
P3V_BAT_SCALED           Normal         3.022      V          N/A          N/A
2.798        3.088
P12V_SCALED              Normal         12.154     V          N/A          N/A
11.623       12.331
P5V_SCALED               Normal         5.036      V          N/A          N/A
4.844        5.157
P3V3_SCALED              Normal         3.318      V          N/A          N/A
3.191        3.381
P5V_STBY_SCALED          Normal         5.109      V          N/A          N/A
4.844        5.157
PV_VCCP_CPU1             Normal         0.950      V          N/A          N/A
0.725        1.391
PV_VCCP_CPU2             Normal         0.891      V          N/A          N/A
0.725        1.391
P1V5_DDR3_CPU1           Normal         1.499      V          N/A          N/A
1.450        1.548
P1V5_DDR3_CPU2           Normal         1.499      V          N/A          N/A
1.450        1.548
P1V1_IOH                 Normal         1.087      V          N/A          N/A
1.068        1.136
P1V8_AUX                 Normal         1.773      V          N/A          N/A
1.744        1.852

Server /sensor #
```

電流センサーの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope sensor**	センサー コマンドモードを開始します。

	コマンドまたはアクション	目的
ステップ 2	Server /sensor # **show current** [**detail**]	サーバの電流センサーの統計情報を表示します。

次に、電流センサーの統計情報を表示する例を示します。

```
Server# scope sensor
Server /sensor # show current
Name                      Sensor Status  Reading    Units      Min. Warning Max. Warning
Min. Failure Max. Failure
------------------------- -------------- ---------- ---------- ------------ ------------
------------ ------------
VR_P2_IMON                Normal         16.00      AMP        N/A          147.20
N/A          164.80
VR_P1_IMON                Normal         27.20      AMP        N/A          147.20
N/A          164.80

Server /sensor #
```

ストレージ センサーの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **show hdd** [**detail**]	ストレージ センサー情報を表示します。

表示されるフィールドについては、次の表で説明します。

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。

次に、ストレージ センサーの情報を表示する例を示します。

```
Server# scope chassis
Server /chassis # show hdd
Name                  Status
--------------------- --------------------
HDD_01_STATUS         present
HDD_02_STATUS         present
HDD_03_STATUS         present
HDD_04_STATUS         present
```

```
Server /chassis #
```

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。

- 仮想 KVM の管理，53 ページ
- 仮想メディアの設定，56 ページ
- Serial over LAN の管理，57 ページ

仮想 KVM の管理

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） KVM コンソールの操作には、GUI 以外は使用できません。 KVM コンソールの起動手順については、『*Cisco UCS C-Series Servers Integrated Management Controller GUI Configuration Guide*』を参照してください。

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope kvm**	KVM コマンド モードを開始します。
ステップ 2	Server /kvm # **set enabled yes**	仮想 KVM をイネーブルにします。
ステップ 3	Server /kvm # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 4	Server /kvm # **show** [**detail**]	（任意）仮想KVMの設定を表示します。

次に、仮想 KVM をイネーブルにする例を示します。

```
Server# scope kvm
Server /kvm # set enabled yes
Server /kvm *# commit
Server /kvm # show
Encryption Enabled Local Video      Active Sessions Enabled KVM Port
------------------ ---------------- --------------- ------- --------
no                 yes              0               yes     2068

Server /kvm #
```

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope kvm**	KVM コマンド モードを開始します。
ステップ 2	Server /kvm # **set enabled no**	仮想 KVM をディセーブルにします。 （注） 仮想 KVM をディセーブルにすると仮想メディア機能へのアクセスがディセーブルになりますが、仮想メディアがイネーブルであれば仮想メディア デバイスは切断されません。
ステップ 3	Server /kvm # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 4	Server /kvm # **show** [**detail**]	（任意）仮想 KVM の設定を表示します。

次に、仮想 KVM をディセーブルにする例を示します。

```
Server# scope kvm
Server /kvm # set enabled no
Server /kvm *# commit
Server /kvm # show
Encryption Enabled Local Video      Active Sessions Enabled KVM Port
------------------ ---------------- --------------- ------- --------
no                 yes              0               no      2068

Server /kvm #
```

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope kvm**	KVM コマンド モードを開始します。
ステップ 2	Server /kvm # **set enabled** {**yes** | **no**}	仮想KVMをイネーブルまたはディセーブルにします。
ステップ 3	Server /kvm # **set encrypted** {**yes** | **no**}	暗号化をイネーブルにすると、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。

	コマンドまたはアクション	目的
ステップ 4	Server /kvm # **set kvm-port** *port*	KVM 通信に使用するポートを指定します。
ステップ 5	Server /kvm # **set local-video** {**yes** | **no**}	ローカル ビデオが [yes] である場合、KVM セッションはサーバに接続されているすべてのモニタにも表示されます。
ステップ 6	Server /kvm # **set max-sessions** *sessions*	許可されている KVM の同時セッションの最大数を指定します。 *sessions* 引数は、1 ～ 4 の範囲の整数になります。
ステップ 7	Server /kvm # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 8	Server /kvm # **show** [**detail**]	（任意）仮想 KVM の設定を表示します。

次に、仮想 KVM を設定し、その設定を表示する例を示します。

```
Server# scope kvm
Server /kvm # set enabled yes
Server /kvm *# set encrypted no
Server /kvm *# set kvm-port 2068
Server /kvm *# set max-sessions 4
Server /kvm *# set local-video yes
Server /kvm *# commit
Server /kvm # show detail
KVM Settings:
    Encryption Enabled: no
    Max Sessions: 4
    Local Video: yes
    Active Sessions: 0
    Enabled: yes
    KVM Port: 2068

Server /kvm #
```

次の作業

GUI から仮想 KVM を起動します。

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope vmedia**	仮想メディア コマンド モードを開始します。
ステップ 2	Server /vmedia # **set enabled** {**yes** | **no**}	仮想メディアをイネーブルまたはディセーブルにします。 デフォルトでは、仮想メディアはディセーブルになります。 （注） 仮想メディアをディセーブルにすると、仮想CD、仮想フロッピー、および仮想HDD デバイスがホストから切断されます。
ステップ 3	Server /vmedia # **set encryption** {**yes** | **no**}	仮想メディアの暗号化をイネーブルまたはディセーブルにします。
ステップ 4	Server /vmedia # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 5	Server /vmedia # **show** [**detail**]	（任意）仮想メディアの設定を表示します。

次に、仮想メディアの暗号化を設定する例を示します。

```
Server# scope vmedia
Server /vmedia # set enabled yes
Server /vmedia *# set encryption yes
Server /vmedia *# commit
Server /vmedia # show detail
vMedia Settings:
    Encryption Enabled: yes
    Enabled: yes
    Max Sessions: 1
    Active Sessions: 0

Server /vmedia #
```

次の作業

KVM を使用して、仮想メディア デバイスをホストに接続します。

Serial over LAN の管理

Serial Over LAN

Serial over LAN（SoL）は、IP を介した SSH セッションを利用して、管理対象システムのシリアル ポートの入力と出力をリダイレクトできるようにするメカニズムです。 SoL は、CIMC 経由でホスト コンソールに到達するための手段となります。

Serial Over LAN に関するガイドラインおよび制約事項

SoL にリダイレクトするには、サーバ コンソールに次の設定が含まれている必要があります。

- シリアル ポート A へのコンソール リダイレクト
- フロー制御なし
- SoL に設定されたのと同じボ ーレート
- VT 100 ターミナル タイプ
- レガシー OS のリダイレクトのディセーブル化

SoL セッションは、ブート メッセージなどの行指向の情報や、BIOS 設定メニューなどの文字指向の画面メニューを表示します。 サーバで Windows などのビットマップ指向表示のオペレーティング システムやアプリケーションが起動されると、SoL セッションによる表示はなくなります。サーバで Linux などのコマンドライン指向の Operating System（OS; オペレーティング システム）が起動された場合、SoL セッションで適切に表示するために OS の追加設定が必要になることがあります。

SoL セッションでは、ファンクション キー F2 を除くキーストロークはコンソールに送信されます。 F2 をコンソールに送信するには、Escape キーを押してから 2 を押します。

Serial over LAN の設定

はじめる前に

Serial over LAN（SoL）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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope sol**	SoL コマンド モードを開始します。
ステップ 2	Server /sol # **set enabled** {**yes** | **no**}	このサーバで SoL をイネーブルまたはディセーブルにします。
ステップ 3	Server /sol # **set baud-rate** {**9600** | **19200** | **38400** | **57600** | **115200**}	システムが SoL 通信に使用するシリアル ボーレートを設定します。 （注） このボー レートは、サーバのシリアル コンソールで設定したボー レートと一致する必要があります。

	コマンドまたはアクション	目的
ステップ 4	Server /sol # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 5	Server /sol # **show** [**detail**]	（任意）SoL の設定を表示します。

次に、SoL を設定する例を示します。

```
Server# scope sol
Server /sol # set enabled yes
Server /sol *# set baud-rate 115200
Server /sol *# commit
Server /sol # show
Enabled Baud Rate(bps)
------- ---------------
yes     115200

Server /sol #
```

Serial Over LAN の起動

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **connect host**	リダイレクトされたサーバ コンソール ポートへの Serial over LAN（SoL）接続を開始します。 このコマンドは、どのコマンド モードでも入力できます。

次の作業

SoL セッションを終了するには、CLI セッションを終了する必要があります。 たとえば、SSH 接続を介した SoL セッションを終了するには、SSH 接続を切断します。

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 の設定，63 ページ
- ユーザ セッションの表示，68 ページ
- ユーザ セッションの終了，68 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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope user** *usernumber*	ユーザ番号 *usernumber* に対するユーザ コマンド モードを開始します。
ステップ 2	Server /user # **set enabled {yes | no}**	CIMC でユーザ アカウントをイネーブルまたはディセーブルにします。
ステップ 3	Server /user # **set name** *username*	ユーザのユーザ名を指定します。
ステップ 4	Server /user # **set password**	パスワードを 2 回入力するように求められます。

	コマンドまたはアクション	目的
ステップ 5	Server /user # **set role** {**readonly** | **user** | **admin**}	ユーザに割り当てるロールを指定します。 ロールには、次のものがあります。 • readonly：こ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：このユーザは、次の操作を実行できます。 • 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：このユーザは、GUI、CLI、IPMI で可能なすべての処理を実行できます。
ステップ 6	Server /user # **commit**	トランザクションをシステムの設定にコミットします。

次に、ユーザ 5 を admin として設定する例を示します。

```
Server# scope user 5
Server /user # set enabled yes
Server /user *# set name john
Server /user *# set password
Please enter password:
Please confirm password:
Server /user *# set role readonly
Server /user *# commit
Server /user #  show
User   Name             Role     Enabled
------ ---------------- -------- --------
5      john             readonly yes
```

Active Directory の設定

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。

Active Directory が CIMC でイネーブルになっている場合、ローカル ユーザ データベースに登録されていないユーザ アカウントに対して Active Directory がユーザ認証とロール許可を実行します。

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

プロパティ	値
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。

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

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

次の作業

CIMC を使用して Active Directory を設定します。

CIMC での Active Directory の設定

ローカル ユーザの認証と許可に Active Directory（AD）サーバを使用するには、CIMC で AD を設定します。

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope ldap**	AD を設定する LDAP コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	Server /ldap # **set enabled** {**yes** | **no**}	ADをイネーブルまたはディセーブルにします。 ADがイネーブルの場合、ローカルユーザデータベースに見つからないユーザ アカウントについて、AD によってユーザ認証とロール許可が実行されます。
ステップ 3	Server /ldap # **set dc***n* *dc-host*	Active Directory ドメイン コントローラ（DC）のホスト名または IP アドレスを指定します。 1 ～ 3 のインデックス *n* 値を使用して最大 3 の DC を指定できます。
ステップ 4	Server /ldap # **set gc***n* *gc-host*	Active Directory グローバル カタログ（GC）サーバのホスト名または IP アドレスを指定します。 1 ～ 3 のインデックス *n* 値を使用して最大 3 の GC を指定できます。
ステップ 5	Server /ldap # **set timeout** *seconds*	LDAP 検索操作がタイムアウトするまで CIMC が待機する秒数を指定します。
ステップ 6	Server /ldap # **set encrypted** {**yes** | **no**}	暗号化がイネーブルである場合、サーバは AD に送信するすべての情報を暗号化します。
ステップ 7	Server /ldap # **set base-dn** *domain-name*	すべてのユーザが属する必要のあるドメインを指定します。
ステップ 8	Server /ldap # **set attribute** *name*	ユーザのロールとロケール情報を保持する LDAP 属性を指定します。 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。 CIMC ユーザ ロールおよびロケールにマップされた既存の LDAP 属性を使用するか、CiscoAVPair 属性など、次の属性 ID を持つカスタム属性を作成できます。 `1.3.6.1.4.1.9.287247.1` （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。
ステップ 9	Server /ldap # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 10	Server /ldap # **show** [**detail**]	（任意）AD の設定を表示します。

次に、CiscoAVPair 属性を使用して AD を設定する例を示します。

```
Server# scope ldap
Server /ldap # set enabled yes
Server /ldap *# set dc1 192.0.20.123
Server /ldap *# set gc1 192.0.20.11
Server /ldap *# set timeout 60
Server /ldap *# set encrypted yes
```

```
Server /ldap *# set base-dn example.com
Server /ldap *# set attribute CiscoAVPair
Server /ldap *# commit
Server /ldap # show detail
LDAP Settings:
    Domain Controller 1: 192.0.20.123
    Domain Controller 2: 0.0.0.0
    Domain Controller 3: 0.0.0.0
    BaseDN: example.com
    Encrypted: yes
    Timeout: 60
    Enabled: yes
    Attribute: CiscoAvPair
    Group Authorization: no
    Global Catalog 1: 192.0.20.11
    Global Catalog 2: 0.0.0.0
    Global Catalog 3: 0.0.0.0

Server /ldap #
```

次の作業

グループの認可に Active Directory グループを使用する場合は、『*Configuring Active Directory Groups in CIMC*』を参照してください。

CIMC での Active Directory グループの設定

（注） Active Directory（AD）グループ許可をイネーブルにして設定すると、ローカル ユーザ データベースに見つからないユーザや Active Directory で CIMC の使用を個別に許可されていないユーザの認証も、ユーザ グループ レベルで実行されます。

はじめる前に

- このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。
- Active Directory（または LDAP）がイネーブル化され、設定されている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope ldap**	AD を設定する LDAP コマンド モードを開始します。
ステップ 2	Server /ldap # **set group-auth** {**yes** | **no**}	AD グループ許可をイネーブルまたはディセーブルにします。
ステップ 3	Server /ldap # **scope role-group** *index*	設定に使用可能な 5 種類のグループ プロファイルのいずれかを選択します。*index* は 1 ～ 5 の数字です。
ステップ 4	Server /ldap/role-group # **set name** *group-name*	サーバへのアクセスが許可された AD データベース内のグループの名前を指定します。

	コマンドまたはアクション	目的
ステップ 5	Server /ldap/role-group # **set domain** *domain-name*	グループが存在する必要がある AD ドメインを指定します。
ステップ 6	Server /ldap/role-group # **set role** {**admin** | **user** | **readonly**}	この AD グループですべてのユーザに割り当てられる権限レベル（ロール）を指定します。次のいずれかになります。 • **admin**：ユーザは使用可能なすべてのアクションを実行できます。 • **user**：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 • **readonly**：ユーザは情報を表示できますが、変更はできません。
ステップ 7	Server /ldap/role-group # **commit**	トランザクションをシステムの設定にコミットします。

次に、AD グループ許可を設定する例を示します。

```
Server# scope ldap
Server /ldap # set group-auth yes
Server /ldap *# scope role-group 5
Server /ldap/role-group *# set name Training
Server /ldap/role-group *# set domain example.com
Server /ldap/role-group *# set role readonly
Server /ldap/role-group *# commit
ucs-c250-M2 /ldap # show role-group
Group  Name              Domain            Role
------ ----------------- ----------------- --------
1      (n/a)             (n/a)             admin
2      (n/a)             (n/a)             user
3      (n/a)             (n/a)             readonly
4      (n/a)             (n/a)             (n/a)
5      Training          example.com       readonly

Server /ldap/role-group #
```

ユーザ セッションの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **show user-session**	現在のユーザ セッションの情報を表示します。

コマンドの出力には、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。

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ている場合、関連付けられたユーザセッションを強制的に終了できるときはこのカラムに [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。

次に、現在のユーザ セッションに関する情報を表示する例を示します。

```
Server# show user-session
ID     Name            IP Address        Type         Killable
------ --------------- ----------------- ------------ --------
15     admin           10.20.30.138      CLI          yes

Server /user #
```

ユーザ セッションの終了

はじめる前に

ユーザセッションを終了するには、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

	コマンドまたはアクション	目的
ステップ 1	Server# **show user-session**	現在のユーザ セッションの情報を表示します。終了するユーザ セッションは、終了可能（killable）であり、独自のセッションではないことが必要です。
ステップ 2	Server /user-session # **scope user-session** *session-number*	終了する番号付きのユーザ セッションに対してユーザ セッション コマンド モードを開始します。
ステップ 3	Server /user-session # **terminate**	ユーザ セッションを終了します。

次に、ユーザ セッション 10 の admin がユーザ セッション 15 を終了する例を示します。

```
Server# show user-session
ID     Name              IP Address         Type          Killable
------ ----------------- ------------------ ------------ --------
10     admin             10.20.41.234       CLI           yes
15     admin             10.20.30.138       CLI           yes
Server# scope user-session 15
Server /user-session # terminate
User session 15 terminated.

Server /user-session #
```

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，71 ページ
- 共通プロパティの設定，74 ページ
- IPv4 の設定，74 ページ
- サーバ VLAN の設定，76 ページ
- ネットワーク セキュリティの設定，77 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

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

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope network**	CIMC ネットワーク コマンド モードを開始します。
ステップ 3	Server /cimc/network # **set mode** {**dedicated** |	NIC モードを次のいずれかに設定します。

	コマンドまたはアクション	目的
	shared_lom | **shared_lom_10g** | **shipping** | **cisco_card**}	• Dedicated：CIMC へのアクセスに管理イーサネット 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）イーサネット ホスト ポートを使用します。 （注） 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。 • Shared LOM 10G：CIMC へのアクセスに 10 G ポートを使用します。 • Shipping：初期接続用の制限付き設定。 通常の操作には、別のモードを選択します。 • 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。
ステップ 4	Server /cimc/network # **set redundancy** {**none** | **active-active** | **active-standby**}	NIC モードが Shared LOM である場合に、NIC 冗長モードを設定します。 冗長モードは、次のいずれかになります。 • none：LOM イーサネット ポートは単独で動作し、問題が生じた場合も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は、すべての LOM イーサネット ポートが利用されます。 • active-standby：1 つの LOM イーサネット ポートに障害が発生すると、トラフィックは別の LOM ポートにフェールオーバーします。
ステップ 5	Server /cimc/network # **commit**	トランザクションをシステムの設定にコミットします。 （注） 使用可能な NIC モードおよび NIC 冗長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。 サーバでサポートされていないモードを選択すると、変更を保存するときにエラー メッセージが表示されます。

次に、CIMC ネットワーク インターフェイスを設定する例を示します。

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set mode dedicated
Server /cimc/network *# commit
```

```
Server /cimc/network #
```

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope network**	CIMC ネットワーク コマンド モードを開始します。
ステップ 3	Server /cimc/network # **set hostname** *host-name*	ホストの名前を指定します。
ステップ 4	Server /cimc/network # **commit**	トランザクションをシステムの設定にコミットします。

次に、コマンドのプロパティを設定する例を示します。

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set hostname Server
Server /cimc/network *# commit
Server /cimc/network #
```

IPv4 の設定

はじめる前に

IPv4 ネットワークの設定を実行するには、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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	Server /cimc # **scope network**	CIMC ネットワーク コマンド モードを開始します。
ステップ 3	Server /cimc/network # **set dhcp-enabled** {**yes** | **no**}	CIMC で DHCP を使用するかどうかを選択します。 （注） DHCP がイネーブルである場合は、CIMC 用に 1 つの IP アドレスを予約するように DHCP サーバを設定することを推奨します。 サーバの複数のポートを通じて CIMC に到達できる場合、それらのポートの全範囲の MAC アドレスに対して 1 つの IP アドレスを予約する必要があります。
ステップ 4	Server /cimc/network # **set v4-addr** *ipv4-address*	CIMC の IP アドレスを指定します。
ステップ 5	Server /cimc/network # **set v4-netmask** *ipv4-netmask*	IP アドレスのサブネット マスクを指定します。
ステップ 6	Server /cimc/network # **set v4-gateway** *gateway-ipv4-address*	IP アドレスのゲートウェイを指定します。
ステップ 7	Server /cimc/network # **set dns-use-dhcp** {**yes** | **no**}	CIMC が DNS サーバ アドレスを DHCP から取得するかどうかを選択します。
ステップ 8	Server /cimc/network # **set preferred-dns-server** *dns1-ipv4-address*	プライマリ DNS サーバの IP アドレスを指定します。
ステップ 9	Server /cimc/network # **set alternate-dns-server** *dns2-ipv4-address*	セカンダリ DNS サーバの IP アドレスを指定します。
ステップ 10	Server /cimc/network # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 11	Server /cimc/network # **show** [**detail**]	（任意）IPv4 ネットワークの設定を表示します。

次に、IPv4 ネットワークの設定を実行し、表示する例を示します。

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # set dhcp-enabled yes
Server /cimc/network *# set v4-addr 10.20.30.11
Server /cimc/network *# set v4-netmask 255.255.248.0
Server /cimc/network *# set v4-gateway 10.20.30.1
Server /cimc/network *# set dns-use-dhcp-enabled no
```

```
Server /cimc/network *# set preferred-dns-server 192.168.30.31
Server /cimc/network *# set alternate-dns-server 192.168.30.32
Server /cimc/network *# commit
Server /cimc/network # show detail
Network Setting:
    IPv4 Address: 10.20.30.11
    IPv4 Netmask: 255.255.248.0
    IPv4 Gateway: 10.20.30.1
    DHCP Enabled: yes
    Obtain DNS Server by DHCP: no
    Preferred DNS: 192.168.30.31
    Alternate DNS: 192.168.30.32
    VLAN Enabled: no
    VLAN ID: 1
    VLAN Priority: 0
    Hostname: Server
    MAC Address: 01:23:45:67:89:AB
    NIC Mode: dedicated
    NIC Redundancy: none

Server /cimc/network #
```

サーバ VLAN の設定

はじめる前に

サーバ VLAN を設定するには、admin としてログインしている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope network**	CIMC ネットワーク コマンドモードを開始します。
ステップ 3	Server /cimc/network # **set vlan-enabled** {**yes** | **no**}	CIMC を VLAN に接続するかどうかを選択します。
ステップ 4	Server /cimc/network # **set vlan-id** *id*	VLAN 番号を指定します。
ステップ 5	Server /cimc/network # **set vlan-priority** *priority*	VLAN でのこのシステムのプライオリティを指定します。
ステップ 6	Server /cimc/network # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 7	Server /cimc/network # **show** [**detail**]	（任意）ネットワークの設定を表示します。

次に、サーバ VLAN を設定する例を示します。

```
Server# scope cimc
Server /cimc # scope network
```

```
Server /cimc/network # set vlan-enabled yes
Server /cimc/network *# set vlan-id 10
Server /cimc/network *# set vlan-priority 32
Server /cimc/network *# commit
Server /cimc/network # show detail
Network Setting:
    IPv4 Address: 10.20.30.11
    IPv4 Netmask: 255.255.248.0
    IPv4 Gateway: 10.20.30.1
    DHCP Enabled: yes
    Obtain DNS Server by DHCP: no
    Preferred DNS: 192.168.30.31
    Alternate DNS: 192.168.30.32
    VLAN Enabled: yes
    VLAN ID: 10
    VLAN Priority: 32
    Hostname: Server
    MAC Address: 01:23:45:67:89:AB
    NIC Mode: dedicated
    NIC Redundancy: none

Server /cimc/network #
```

ネットワーク セキュリティの設定

ネットワーク セキュリティ

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	Server /cimc # **scope network**	CIMC ネットワーク コマンド モードを開始します。
ステップ 3	Server /cimc/network # **scope ipblocking**	IP ブロッキング コマンド モードを開始します。
ステップ 4	Server /cimc/network/ipblocking # **set enabled** {**yes** | **no**}	IP ブロッキングをイネーブルまたはディセーブルにします。
ステップ 5	Server /cimc/network/ipblocking # **set fail-count** *fail-count*	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を設定します。 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。
ステップ 6	Server /cimc/network/ipblocking # **set fail-window** *fail-seconds*	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）を設定します。 60 ～ 120 の範囲の整数を入力します。
ステップ 7	Server /cimc/network/ipblocking # **set penalty-time** *penalty-seconds*	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を設定します。 300 ～ 900 の範囲の整数を入力します。
ステップ 8	Server /cimc/network/ipblocking # **commit**	トランザクションをシステムの設定にコミットします。

次に、IP ブロッキングを設定する例を示します。

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # scope ipblocking
Server /cimc/network/ipblocking # set enabled yes
Server /cimc/network/ipblocking *# set fail-count 5
Server /cimc/network/ipblocking *# set fail-window 90
Server /cimc/network/ipblocking *# set penalty-time 600
Server /cimc/network/ipblocking *# commit
Server /cimc/network/ipblocking #
```

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，79 ページ
- ネットワーク アダプタのプロパティの表示，80 ページ
- ネットワーク アダプタのプロパティの設定，81 ページ
- vHBA の管理，82 ページ
- vNIC の管理，96 ページ
- VM FEX の管理，106 ページ
- アダプタ設定のバックアップと復元，113 ページ
- アダプタ ファームウェアの管理，115 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設置される場合にのみ使用できます。

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

- Cisco UCS P81E 仮想インターフェイス カード

Cisco UCS P81E 仮想インターフェイス カード

Cisco UCS P81E 仮想インターフェイス カードは、仮想化された環境、物理環境のモビリティ強化を求めている組織、および NIC、HBA、ケーブル配線、スイッチの減少によるコスト削減と管理

オーバーヘッドの軽減を目指しているデータセンターに対して最適化されています。 Fibre Channel over Ethernet（FCoE）PCIe カードには、次の利点があります。

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

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

ネットワーク アダプタのプロパティの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **show adapter** [*index*] [**detail**]	アダプタのプロパティを表示します。 1 つのアダプタのプロパティを表示するには、*index* 引数として PCI スロット番号を指定します。

次に、アダプタ 1 のプロパティを表示する例を示します。

```
Server# scope chassis
Server /chassis # show adapter
PCI Slot Product Name   Serial Number  Product ID     Vendor
-------- -------------- -------------- -------------- --------------------
1        UCS VIC P81E   QCI1424A540    N2XX-ACPCI01   Cisco Systems Inc

Server /chassis # show adapter 1 detail
PCI Slot 1:
    Product Name: UCS VIC P81E
    Serial Number: QCI1424A540
    Product ID: N2XX-ACPCI01
    Adapter Hardware Revision: 4
    Current FW Version: 1.2(0.33)
    NIV: Disabled
    FIP: Enabled
    Configuration Pending: no
    CIMC Management Enabled : no
    VID: V00
```

```
    Vendor: Cisco Systems Inc
    Description:
    FW Image 1 Version: 1.2(0.33)
    FW Image 1 State: RUNNING ACTIVATED
    FW Image 2 Version: 1.4(0.290)
    FW Image 2 State: BACKUP INACTIVATED
    FW Update Status: Idle
    FW Update Error: No error
    FW Update Stage: No operation (0%)
    FW Update Overall Progress: 0%

Server /chassis #
```

ネットワーク 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、admin 権限を持っ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 カードがシャーシに装着され、サーバの電源がオンになっている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **show adapter**	（任意）使用可能なアダプタ デバイスを表示します。
ステップ 3	Server /chassis # **scope adapter** *index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンドモードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。
ステップ 4	Server /chassis/adapter # **set fip-mode** {**disable** | **enable**}	アダプタ カードで FCoE Initialization Protocol（FIP）をイネーブルまたはディセーブルにします。 FIP はデフォルトで有効になっています。 （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、このオプションをディセーブルにすることを推奨します。
ステップ 5	Server /chassis/adapter # **set niv-mode** {**disable** | **enable**}	アダプタ カードで Network Interface Virtualization（NIV）をイネーブルまたはディセーブルにします。 NIV はデフォルトで無効になっています。 NIV モードがイネーブルな場合、vNIC は以下の操作を実行できます。

	コマンドまたはアクション	目的
		• 特定のチャネルに割り当てることができます • ポート プロファイルに関連付けることができます • 通信の問題がある場合に別の vNIC にフェールオーバーできます
ステップ 6	Server /chassis/adapter # **configure-vmfex** *port-count*	NIV モードがイネーブルの場合、*port-count* には CIMC を使用して作成する VM FEX インターフェイスの数を 0 ～ 112 の範囲で指定します。
ステップ 7	Server /chassis/adapter # **commit**	トランザクションをシステムの設定にコミットします。

次に、アダプタ 1 のプロパティを設定する例を示します。

```
Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # set fip-mode enable
Server /chassis/adapter *# commit
Server /chassis/adapter #
```

vHBA の管理

vHBA 管理のガイドライン

vHBA を管理する場合は、次のガイドラインと制限事項を考慮してください。

- Cisco UCS P81E 仮想インターフェイス カードには 2 つの vHBA（fc0 と 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になっている場合は、vHBA を作成するときにチャネル番号を割り当てる必要があります。

- FCoE アプリケーションで Cisco UCS P81E 仮想インターフェイス カードを使用する場合は、vHBA を FCoE VLAN に関連付ける必要があります。vHBA のプロパティの変更，（84 ページ）の説明に従って FCoE VLAN を割り当ててください。
- 設定の変更後は、その設定を有効にするためにホストをリブートする必要があります。

vHBA のプロパティの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scope adapter** *index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンド モードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。
ステップ 3	Server /chassis/adapter # **show host-fc-if** [**fc0** | **fc1** | *name*] [**detail**]	指定した単一の vHBA またはすべての vHBA のプロパティを表示します。

次に、アダプタ カード 1 上のすべての vHBA および fc0 の詳細なプロパティを表示する例を示します。

```
Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # show host-fc-if
Name     World Wide Port Name     FC SAN Boot Uplink Port
-------- ----------------------- ----------- -----------
fc0      20:00:00:22:BD:D6:5C:35  Disabled    0
fc1      20:00:00:22:BD:D6:5C:36  Disabled    1

Server /chassis/adapter # show host-fc-if fc0 detail
Name fc0:
    World Wide Node Name: 10:00:00:22:BD:D6:5C:35
    World Wide Port Name: 20:00:00:22:BD:D6:5C:35
    FC SAN Boot: Disabled
    Persistent LUN Binding: Disabled
    Uplink Port: 0
    MAC Address: 00:22:BD:D6:5C:35
    CoS: 3
    VLAN: NONE
    Rate Limiting: OFF
    PCIe Device Order: ANY
    EDTOV: 2000
    RATOV: 10000
    Maximum Data Field Size: 2112
    Channel Number: 3
    Port Profile:

Server /chassis/adapter #
```

vHBA のプロパティの変更

はじめる前に

このタスクを実行するには、admin 権限を持ってログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **show adapter**	（任意）使用可能なアダプタ デバイスを表示します。
ステップ 3	Server /chassis # **scope adapter** *index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンド モードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。
ステップ 4	Server /chassis/adapter # **scope host-fc-if** {**fc0** | **fc1** | *name*}	指定した vHBA に対してホスト ファイバ チャネル インターフェイス コマンド モードを開始します。
ステップ 5	Server /chassis/adapter/host-fc-if # **set wwnn** *wwnn*	アダプタの一意のワールド ワイド ノード名（WWNN）を hh:hh:hh:hh:hh:hh:hh:hh の形式で指定します。 このコマンドで指定しない場合、WWNN はシステムによって自動的に生成されます。
ステップ 6	Server /chassis/adapter/host-fc-if # **set wwpn** *wwpn*	アダプタの一意のワールド ワイド ポート名（WWPN）を hh:hh:hh:hh:hh:hh:hh:hh の形式で指定します。 このコマンドで指定しない場合、WWPN はシステムによって自動的に生成されます。
ステップ 7	Server /chassis/adapter/host-fc-if # **set boot** {**disable** | **enable**}	FC SAN ブートを有効または無効にします。デフォルトはディセーブルです。
ステップ 8	Server /chassis/adapter/host-fc-if # **set persistent-lun-binding** {**disable** | **enable**}	永続的な LUN バインディングを有効または無効にします。 デフォルトはディセーブルです。
ステップ 9	Server /chassis/adapter/host-fc-if # **set mac-addr** *mac-addr*	vHBA の MAC アドレスを指定します。

	コマンドまたはアクション	目的
ステップ 10	Server /chassis/adapter/host-fc-if # **set vlan** {**none** | *vlan-id*}	この vHBA のデフォルトの VLAN を指定します。 有効な VLAN 番号は 1 ～ 4094 です。デフォルトは none です。
ステップ 11	Server /chassis/adapter/host-fc-if # **set cos** *cos-value*	受信パケットにマークされるサービス クラス（CoS）値を指定します。この設定は、vHBA がホスト CoS を信頼するように設定されていない場合に限り有効です。 有効な CoS 値は 0 ～ 6 です。デフォルトは 0 です。 値が大きいほど重要なトラフィックであることを意味します。 この設定は NIV モードでは機能しません。
ステップ 12	Server /chassis/adapter/host-fc-if # **set rate-limit** {**off** | *rate*}	vHBA の最大データ レートを指定します。 指定できる範囲は 1 ～ 10000 Mbps です。デフォルトは off です。 この設定は NIV モードでは機能しません。
ステップ 13	Server /chassis/adapter/host-fc-if # **set order** {**any** | *0-99*}	PCIe バスのデバイス番号割り当てについて、このデバイスの相対順序を指定します。デフォルトは any です。
ステップ 14	Server /chassis/adapter/host-fc-if # **set error-detect-timeout** *msec*	Error Detect TimeOut Value（EDTOV）を指定します。エラーが発生したとシステムが見なすまでに待機するミリ秒数です。 指定できる値の範囲は、1000 ～ 100000 です。デフォルトは、2000 ミリ秒です。
ステップ 15	Server /chassis/adapter/host-fc-if # **set resource-allocation-timeout** *msec*	Resource Allocation TimeOut Value（RATOV）を指定します。リソースを適切に割り当てることができないとシステムが見なすまでに待機するミリ秒数です。 指定できる値の範囲は、5000 ～ 100000 です。デフォルトは、10000 ミリ秒です。
ステップ 16	Server /chassis/adapter/host-fc-if # **set max-field-size** *size*	vHBA がサポートするファイバ チャネル フレーム ペイロードの最大サイズ（バイト数）を指定します。 指定できる値の範囲は 1 ～ 2112 です。デフォルトは 2112 バイトです。
ステップ 17	Server /chassis/adapter/host-fc-if # **scope error-recovery**	ファイバ チャネル エラー回復コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 18	Server /chassis/adapter/host-fc-if/error-recovery # **set fcp-error-recovery** {**disable** | **enable**}	FCP エラー回復を有効または無効にします。デフォルトはディセーブルです。
ステップ 19	Server /chassis/adapter/host-fc-if/error-recovery # **set link-down-timeout** *msec*	リンク ダウン タイムアウト値を指定します。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です。指定できる値の範囲は、0 ～ 240000 です。デフォルトは、30000 ミリ秒です。
ステップ 20	Server /chassis/adapter/host-fc-if/error-recovery # **set port-down-io-retry-count** *count*	ポート ダウン I/O 再試行回数値を指定します。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です。 指定できる値の範囲は、0 ～ 255 です。デフォルトは、8 回です。
ステップ 21	Server /chassis/adapter/host-fc-if/error-recovery # **set port-down-timeout** *msec*	ポート ダウン タイムアウト値を指定します。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です。 指定できる値の範囲は、0 ～ 240000 です。デフォルトは、10000 ミリ秒です。
ステップ 22	Server /chassis/adapter/host-fc-if/error-recovery # **exit**	ホスト ファイバ チャネル インターフェイス コマンド モードを終了します。
ステップ 23	Server /chassis/adapter/host-fc-if # **scope interrupt**	割り込みコマンド モードを開始します。
ステップ 24	Server /chassis/adapter/host-fc-if/interrupt # **set interrupt-mode** {**intx** | **msi** | **msix**}	ファイバチャネル割り込みモードを指定します。 次のモードがあります。 • **intx**：ラインベースの割り込み（INTx） • **msi**：メッセージ シグナル割り込み（MSI） • **msix**：機能拡張されたメッセージ シグナル割り込み（MSIx）。 これは推奨オプションであり、デフォルトになっています。

	コマンドまたはアクション	目的
ステップ 25	Server /chassis/adapter/host-fc-if/interrupt # **exit**	ホスト ファイバ チャネル インターフェイス コマンド モードを終了します。
ステップ 26	Server /chassis/adapter/host-fc-if # **scope port**	ファイバ チャネル ポート コマンド モードを開始します。
ステップ 27	Server /chassis/adapter/host-fc-if/port # **set outstanding-io-count** *count*	I/O スロットル数を指定します。vHBA 内に同時に保留可能な I/O 操作の数です。 指定できる値の範囲は、1 ～ 1024 です。デフォルトは、512 個の操作です。
ステップ 28	Server /chassis/adapter/host-fc-if/port # **set max-target-luns** *count*	ターゲットあたりの論理ユニット番号（LUN）の最大数を指定します。ドライバで検出される LUN の最大数です。 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。指定できる値の範囲は、1 ～ 1024 です。デフォルトは、256 個の LUN です。
ステップ 29	Server /chassis/adapter/host-fc-if/port # **exit**	ホスト ファイバ チャネル インターフェイス コマンド モードを終了します。
ステップ 30	Server /chassis/adapter/host-fc-if # **scope port-f-logi**	ファイバ チャネル ファブリック ログイン コマンド モードを開始します。
ステップ 31	Server /chassis/adapter/host-fc-if/port-f-logi # **set flogi-retries** {**infinite** | *count*}	ファブリック ログイン（FLOGI）の再試行回数値を指定します。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です。 0 ～ 4294967295 の数値を入力するか、**infinite** を入力します。デフォルトは無限（infinite）の再試行です。
ステップ 32	Server /chassis/adapter/host-fc-if/port-f-logi # **set flogi-timeout** *msec*	ファブリック ログイン（FLOGI）タイムアウト値を指定します。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です。 指定できる値の範囲は、1 ～ 255000 です。デフォルトは、2000 ミリ秒です。
ステップ 33	Server /chassis/adapter/host-fc-if/port-f-logi # **exit**	ホスト ファイバ チャネル インターフェイス コマンド モードを終了します。
ステップ 34	Server /chassis/adapter/host-fc-if # **scope port-p-logi**	ファイバ チャネル ポート ログイン コマンド モードを開始します。
ステップ 35	Server /chassis/adapter/host-fc-if/port-p-logi # **set plogi-retries** *count*	ポート ログイン（PLOGI）の再試行回数値を指定します。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

	コマンドまたはアクション	目的
		です。指定できる値の範囲は、0～255 です。デフォルトは、8 回です。
ステップ 36	Server /chassis/adapter/host-fc-if/port-p-logi # **set plogi-timeout** *msec*	ポートログイン（PLOGI）タイムアウト値を指定します。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です。指定できる値の範囲は、1 ～ 255000 です。デフォルトは、2000 ミリ秒です。
ステップ 37	Server /chassis/adapter/host-fc-if/port-p-logi # **exit**	ホスト ファイバ チャネル インターフェイス コマンド モードを終了します。
ステップ 38	Server /chassis/adapter/host-fc-if # **scope scsi-io**	SCSI I/O コマンド モードを開始します。
ステップ 39	Server /chassis/adapter/host-fc-if/scsi-io # **set cdb-wq-count** *count*	割り当てる Command Descriptor Block（CDB）送信キュー リソースの数です。指定できる値の範囲は 1 ～ 8 です。デフォルトは 1 です。
ステップ 40	Server /chassis/adapter/host-fc-if/scsi-io # **set cdb-wq-ring-size** *size*	Command Descriptor Block（CDB）送信キュー内の記述子の数。指定できる値の範囲は 64 ～ 512 です。デフォルトは 512 です。
ステップ 41	Server /chassis/adapter/host-fc-if/scsi-io # **exit**	ホスト ファイバ チャネル インターフェイス コマンド モードを終了します。
ステップ 42	Server /chassis/adapter/host-fc-if # **scope trans-queue**	ファイバ チャネル送信キュー コマンド モードを開始します。
ステップ 43	Server /chassis/adapter/host-fc-if/trans-queue # **set fc-wq-ring-size** *size*	ファイバ チャネル送信キュー内の記述子の数。指定できる値の範囲は 64 ～ 128 です。デフォルトは 64 です。
ステップ 44	Server /chassis/adapter/host-fc-if/trans-queue # **exit**	ホスト ファイバ チャネル インターフェイス コマンド モードを終了します。
ステップ 45	Server /chassis/adapter/host-fc-if # **scope recv-queue**	ファイバ チャネル受信キュー コマンド モードを開始します。
ステップ 46	Server /chassis/adapter/host-fc-if/recv-queue # **set fc-rq-ring-size** *size*	ファイバ チャネル受信キュー内の記述子の数。指定できる値の範囲は 64 ～ 128 です。デフォルトは 64 です。
ステップ 47	Server /chassis/adapter/host-fc-if/recv-queue # **exit**	ホスト ファイバ チャネル インターフェイス コマンド モードを終了します。

	コマンドまたはアクション	目的
ステップ 48	Server /chassis/adapter/host-fc-if # **commit**	トランザクションをシステムの設定にコミットします。 （注） 変更した内容は、サーバを次にリブートしたときに有効になります。

次の例では、vHBA のプロパティを設定しています。

```
Server# scope chassis
Server /chassis # show adapter
PCI Slot Product Name   Serial Number  Product ID     Vendor
-------- -------------- -------------- -------------- --------------------
1        UCS VIC P81E   QCI1417A0QK    N2XX-ACPCI01   Cisco Systems Inc

Server /chassis # scope adapter 1
Server /chassis/adapter # scope host-fc-if fc1
Server /chassis/adapter/host-fc-if # set boot enable
Server /chassis/adapter/host-fc-if *# scope scsi-io
Server /chassis/adapter/host-fc-if/scsi-io *# set cdb-wq-count 2
Server /chassis/adapter/host-fc-if/scsi-io *# exit
Server /chassis/adapter/host-fc-if *# commit
Server /chassis/adapter/host-fc-if #
```

次の作業

サーバをリブートして変更を適用します。

vHBA の作成

このアダプタには、永続的な vHBA が 2 つあります。 NIV モードがイネーブルの場合、16 まで vHBA を追加作成できます。

はじめる前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scope adapter** *index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンド モードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。

	コマンドまたはアクション	目的
ステップ 3	Server /chassis/adapter # **create host-fc-if** *name*	vHBA を作成し、ホストのファイバ チャネル インターフェイスのコマンドモードを開始します。 *name* 引数には最大 32 文字の ASCII 文字を使用できます。
ステップ 4	Server /chassis/adapter/host-fc-if # **set channel-number** *number*	（任意） アダプタで NIV モードがイネーブルになっている場合、この vHBA にチャネル番号を割り当てる必要があります。 指定できる範囲は 1 ～ 1000 です。
ステップ 5	Server /chassis/adapter/host-fc-if # **commit**	トランザクションをシステムの設定にコミットします。 （注） 変更した内容は、サーバを次にリブートしたときに有効になります。

次に、アダプタ 1 の vHBA を作成する例を示します。

```
Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # create host-fc-if Vhba5
Server /chassis/adapter/host-fc-if *# commit
New host-fc-if settings will take effect upon the next server reset
Server /chassis/adapter/host-fc-if #
```

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, （84 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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scope adapter** *index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンドモードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。

	コマンドまたはアクション	目的
ステップ 3	Server /chassis/adapter # **delete host-fc-if** *name*	指定された vHBA を削除します。 （注） 2 つのデフォルトの vHBA である [fc0] または [fc1] は削除できません。
ステップ 4	Server /chassis/adapter # **commit**	トランザクションをシステムの設定にコミットします。 （注） 変更した内容は、サーバを次にリブートしたときに有効になります。

次に、アダプタ 1 の vHBA を削除する例を示します。

```
Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # delete host-fc-if Vhba5
Server /chassis/adapter *# commit
Server /chassis/adapter #
```

vHBA ブート テーブル

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

ブート テーブルの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scope adapter** *index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンド モードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。
ステップ 3	Server /chassis/adapter # **scope host-fc-if** {**fc0** | **fc1** | *name*}	指定した vHBA に対してホスト ファイバ チャネル インターフェイス コマンド モードを開始します。
ステップ 4	Server /chassis/adapter/host-fc-if # **show boot**	ファイバチャネルインターフェイスのブートテーブルを表示します。

次に、vHBA のブート テーブルを表示する例を示します。

```
Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # scope host-fc-if fc1
Server /chassis/adapter/host-fc-if # show boot
Boot Table Entry  Boot Target WWPN           Boot LUN ID
----------------- -------------------------- ------------
0                 20:00:00:11:22:33:44:55    3
1                 20:00:00:11:22:33:44:56    5

Server /chassis/adapter/host-fc-if #
```

ブート テーブル エントリの作成

最大 4 個のブート テーブル エントリを作成できます。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scope adapter** *index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンド モードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。
ステップ 3	Server /chassis/adapter # **scope host-fc-if** {**fc0** | **fc1** | *name*}	指定した vHBA に対してホスト ファイバ チャネル インターフェイス コマンド モードを開始します。
ステップ 4	Server /chassis/adapter/host-fc-if # **create-boot-entry** *wwpn lun-id*	ブート テーブル エントリを作成します。 • *wwpn*：ブート ターゲットの「hh:hh:hh:hh:hh:hh:hh:hh」形式の World Wide Port Name（WWPN）。 • *lun-id*：ブート LUN の LUN ID。 指定できる範囲は 0 ～ 255 です。
ステップ 5	Server /chassis/adapter/host-fc-if # **commit**	トランザクションをシステムの設定にコミットします。 （注） 変更した内容は、サーバを次にリブートしたときに有効になります。

次に、vHBA fc1 のブート テーブル エントリを作成する例を示します。

```
Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # scope host-fc-if fc1
Server /chassis/adapter/host-fc-if # create-boot-entry 20:00:00:11:22:33:44:55 3
Server /chassis/adapter/host-fc-if *# commit
New boot table entry will take effect upon the next server reset
Server /chassis/adapter/host-fc-if #
```

ブート テーブル エントリの削除

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scope adapter** *index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンド モードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。
ステップ 3	Server /chassis/adapter # **scope host-fc-if** {**fc0** | **fc1** | *name*}	指定した vHBA に対してホスト ファイバ チャネル インターフェイス コマンド モードを開始します。
ステップ 4	Server /chassis/adapter/host-fc-if # **show boot**	ブート テーブルを表示します。 ブート テーブル エントリ フィールドから、削除するエントリの番号を探します。
ステップ 5	Server /chassis/adapter/host-fc-if # **delete boot** *entry*	テーブルの指定した位置からブート テーブル エントリを削除します。 *entry* の範囲は 0 ～ 3 です。 変更は、サーバを次にリセットしたときに有効になります。
ステップ 6	Server /chassis/adapter/host-fc-if # **commit**	トランザクションをシステムの設定にコミットします。 （注） 変更した内容は、サーバを次にリブートしたときに有効になります。

次に、vHBA fc1 のブート テーブル エントリ番号 1 を削除する例を示します。

```
Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # scope host-fc-if fc1
Server /chassis/adapter/host-fc-if # show boot
Boot Table Entry  Boot Target WWPN           Boot LUN ID
----------------- -------------------------- ------------
0                 20:00:00:11:22:33:44:55    3
```

```
1                20:00:00:11:22:33:44:56    5

Server /chassis/adapter/host-fc-if # delete boot 1
Server /chassis/adapter/host-fc-if *# commit
New host-fc-if settings will take effect upon the next server reset
Server /chassis/adapter/host-fc-if # show boot
Boot Table Entry  Boot Target WWPN           Boot LUN ID
----------------- ------------------------- ------------
0                 20:00:00:11:22:33:44:55    3

Server /chassis/adapter/host-fc-if #
```

次の作業

サーバをリブートして変更を適用します。

vHBA の永続的なバインディング

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

永続的なバインディングのイネーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scope adapter** *index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンド モードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。
ステップ 3	Server /chassis/adapter # **scope host-fc-if** {**fc0** | **fc1** | *name*}	指定した vHBA に対してホスト ファイバ チャネル インターフェイス コマンド モードを開始します。
ステップ 4	Server /chassis/adapter/host-fc-if # **scope perbi**	vHBA の永続的なバインディングのコマンド モードを開始します。
ステップ 5	Server /chassis/adapter/host-fc-if/perbi # **set persistent-lun-binding enable**	vHBA の永続的なバインディングをイネーブルにします。
ステップ 6	Server /chassis/adapter/host-fc-if/perbi # **commit**	トランザクションをシステムの設定にコミットします。

次に、vHBA の永続的なバインディングをイネーブルにする例を示します。

```
Server# scope chassis
Server /chassis # scope adapter 4
Server /chassis/adapter # scope host-fc-if fc1
Server /chassis/adapter/host-fc-if # scope perbi
Server /chassis/adapter/host-fc-if/perbi # set persistent-lun-binding enable
Server /chassis/adapter/host-fc-if/perbi *# commit
Server /chassis/adapter/host-fc-if/perbi #
```

永続的なバインディングのディセーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scope adapter** *index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンド モードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。
ステップ 3	Server /chassis/adapter # **scope host-fc-if** {**fc0** | **fc1** | *name*}	指定した vHBA に対してホスト ファイバ チャネル インターフェイス コマンド モードを開始します。
ステップ 4	Server /chassis/adapter/host-fc-if # **scope perbi**	vHBA の永続的なバインディングのコマンド モードを開始します。
ステップ 5	Server /chassis/adapter/host-fc-if/perbi # **set persistent-lun-binding disable**	vHBA の永続的なバインディングをディセーブルにします。
ステップ 6	Server /chassis/adapter/host-fc-if/perbi # **commit**	トランザクションをシステムの設定にコミットします。

次に、vHBA の永続的なバインディングをディセーブルにする例を示します。

```
Server# scope chassis
Server /chassis # scope adapter 4
Server /chassis/adapter # scope host-fc-if fc1
Server /chassis/adapter/host-fc-if # scope perbi
Server /chassis/adapter/host-fc-if/perbi # set persistent-lun-binding disable
Server /chassis/adapter/host-fc-if/perbi *# commit
Server /chassis/adapter/host-fc-if/perbi #
```

永続的なバインディングの再構築

はじめる前に

vHBA のプロパティで永続的なバインディングをイネーブルにする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scope adapter** *index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンドモードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。
ステップ 3	Server /chassis/adapter # **scope host-fc-if** {**fc0** | **fc1** | *name*}	指定した vHBA に対してホスト ファイバ チャネル インターフェイス コマンド モードを開始します。
ステップ 4	Server /chassis/adapter/host-fc-if # **scope perbi**	vHBA の永続的なバインディングのコマンドモードを開始します。
ステップ 5	Server /chassis/adapter/host-fc-if/perbi # **rebuild**	vHBA の永続的なバインディング テーブルを再構築します。

次に、vHBA の永続的なバインディング テーブルを再構築する例を示します。

```
Server# scope chassis
Server /chassis # scope adapter 4
Server /chassis/adapter # scope host-fc-if fc1
Server /chassis/adapter/host-fc-if # scope perbi
Server /chassis/adapter/host-fc-if/perbi # rebuild

Server /chassis/adapter/host-fc-if/perbi #
```

vNIC の管理

vNIC 管理のガイドライン

vNIC を管理する場合は、次のガイドラインと制限事項を考慮してください。

- Cisco UCS P81E 仮想インターフェイス カードには 2 つのデフォルト vNIC（eth0 と eth1）があります。 最大 16 個の vNIC を作成してこのアダプタ カードに追加することができます。

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

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

vNIC のプロパティの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scope adapter** *index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンド モードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。
ステップ 3	Server /chassis/adapter # **show host-eth-if** [**eth0** | **eth1** | *name*] [**detail**]	指定した単一の vNIC またはすべての vNIC のプロパティを表示します。

次に、すべての vNIC の簡単なプロパティと eth0 の詳細プロパティを表示する例を示します。

```
Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # show host-eth-if
Name     MTU  Uplink Port MAC Address       CoS VLAN PXE Boot
-------- ---- ----------- ----------------- --- ---- --------
eth0     1500 0           00:22:BD:D6:5C:33 0   NONE Enabled
eth1     1500 1           00:22:BD:D6:5C:34 0   NONE Enabled

Server /chassis/adapter # show host-eth-if eth0 detail
Name eth0:
    MTU: 1500
    Uplink Port: 0
    MAC Address: 00:22:BD:D6:5C:33
    CoS: 0
    Trust Host CoS: disabled
    PCI Order: ANY
    VLAN: NONE
    VLAN Mode: TRUNK
    Rate Limiting: OFF
    PXE Boot: enabled
    Channel Number: N/A
```

```
    Port Profile: N/A
    Uplink Failover: N/A
    Uplink Failback Timeout: N/A

Server /chassis/adapter #
```

vNIC のプロパティの変更

はじめる前に

このタスクを実行するには、admin 権限を持ってログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **show adapter**	（任意）使用可能なアダプタ デバイスを表示します。
ステップ 3	Server /chassis # **scope adapter** *index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンド モードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。
ステップ 4	Server /chassis/adapter # **scope host-eth-if** {**eth0** | **eth1** | *name*}	指定した vNIC に対してホスト イーサネット インターフェイス コマンド モードを開始します。
ステップ 5	Server /chassis/adapter/host-eth-if # **set mtu** *mtu-value*	vNIC で受け入れられる Maximum Transmission Unit（MTU）またはパケット サイズを指定します。 有効な MTU 値は 1500 ～ 9000 バイトです。デフォルトは 1500 です。
ステップ 6	Server /chassis/adapter/host-eth-if # **set uplink** {**0** | **1**}	この vNIC に関連付けられているアップリンク ポートを指定します。 この vNIC に対するすべてのトラフィックは、このアップリンク ポートを通過します。
ステップ 7	Server /chassis/adapter/host-eth-if # **set mac-addr** *mac-addr*	hh:hh:hh:hh:hh:hh または hhhh:hhhh:hhhh の形式で vNIC の MAC アドレスを指定します。
ステップ 8	Server /chassis/adapter/host-eth-if # **set cos** *cos-value*	受信パケットにマークされるサービス クラス（CoS）値を指定します。この設定は、vNIC がホスト CoS を信頼するように設定されていない場合に限り有効です。 有効な CoS 値は 0 ～ 6

	コマンドまたはアクション	目的
		です。デフォルトは 0 です。 値が大きいほど重要なトラフィックであることを意味します。 （注） NIV がイネーブルの場合、この設定はスイッチによって決定され、コマンドは無視されます。
ステップ 9	Server /chassis/adapter/host-eth-if # **set trust-host-cos** {**disable** | **enable**}	vNIC がホスト CoS を信頼するか、パケットを再マーキングするかを指定します。 動作は次のようになります。 • **disable**：受信パケットは設定済み CoS と再マーキングされます。 これはデフォルトです。 • **enable**：インバウンド パケット（ホスト CoS）の既存の CoS 値が保持されます。
ステップ 10	Server /chassis/adapter/host-eth-if # **set order** {**any** | *0-99*}	PCI バスのデバイス番号割り当てについて、このデバイスの相対順序を指定します。デフォルトは any です。
ステップ 11	Server /chassis/adapter/host-eth-if # **set vlan** {**none** | *vlan-id*}	この vNIC のデフォルトの VLAN を指定します。 有効な VLAN 番号は 1 ～ 4094 です。デフォルトは none です。 （注） NIV がイネーブルの場合、この設定はスイッチによって決定され、コマンドは無視されます。
ステップ 12	Server /chassis/adapter/host-eth-if # **set vlan-mode** {**access** | **trunk**}	vNIC に VLAN モードを指定します。 次のモードがあります。 • **access**：vNIC は 1 つの VLAN だけに属します。 • **trunk**：vNIC は複数の VLAN に属することができます。 これはデフォルトです。 （注） NIV がイネーブルの場合、この設定はスイッチによって決定され、コマンドは無視されます。
ステップ 13	Server /chassis/adapter/host-eth-if # **set rate-limit** {**off** | *rate*}	vNIC の最大データ レートを指定します。 指定できる範囲は 1 ～ 10000 Mbps です。デフォルトは off です。

	コマンドまたはアクション	目的
		（注） NIV がイネーブルの場合、この設定はスイッチによって決定され、コマンドは無視されます。
ステップ 14	Server /chassis/adapter/host-eth-if # **set boot** {**disable** | **enable**}	vNIC を使用して PXE ブートを実行するかどうかを指定します。 デフォルトでは、2 つのデフォルト vNIC に対してはイネーブル、ユーザ作成の vNIC に対してはディセーブルです。
ステップ 15	Server /chassis/adapter/host-eth-if # **set channel-number** *number*	アダプタに対して NIV モードがイネーブルである場合、この vNIC に割り当てられるチャネル番号を選択します。 指定できる範囲は 1 ～ 1000 です。
ステップ 16	Server /chassis/adapter/host-eth-if # **set port-profile** *name*	アダプタに対して NIV モードがイネーブルである場合、vNIC に関連付けられるポート プロファイルを選択します。 （注） *name* は、このサーバが接続されているスイッチに定義されているポート プロファイルである必要があります。
ステップ 17	Server /chassis/adapter/host-eth-if # **set uplink-failover** {**disable** | **enable**}	アダプタに対して NIV モードがイネーブルである場合、通信問題が発生したときにこの vNIC 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ようにするには、この設定をイネーブルにします。
ステップ 18	Server /chassis/adapter/host-eth-if # **set uplink-failback-timeout** *seconds*	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。 *seconds* に 0 ～ 600 の範囲の秒数を入力します。
ステップ 19	Server /chassis/adapter/host-eth-if # **scope interrupt**	割り込みコマンド モードを開始します。
ステップ 20	Server /chassis/adapter/host-eth-if/interrupt # **set interrupt-count** *count*	割り込みリソースの数を指定します。 指定できる値の範囲は、1 ～ 514 です。デフォルトは、8 です。 通常は、完了キューごとに 1 つの割り込みリソースを割り当てる必要があります。
ステップ 21	Server /chassis/adapter/host-eth-if/interrupt # **set coalescing-time** *usec*	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。

	コマンドまたはアクション	目的
		指定できる範囲は 1 ～ 65535 ミリ秒です。デフォルト値は125ミリ秒です。 調停をオフにするには、0（ゼロ）を入力します。
ステップ 22	Server /chassis/adapter/host-eth-if/interrupt # **set coalescing-type** {**idle** | **min**}	調停には次のタイプがあります。 • **idle**：アクティビティなしの期間が少なくとも調停時間設定に指定された時間内は、システムから割り込み送信されません。 • **min**：システムは、別の割り込みイベントを送信する前に、調停時間設定に指定された時間だけ待機します。 これはデフォルトです。
ステップ 23	Server /chassis/adapter/host-eth-if/interrupt # **set interrupt-mode** {**intx** | **msi** | **msix**}	イーサネット割り込みモードを指定します。 次のモードがあります。 • **intx**：ラインベースの割り込み（PCI INTx） • **msi**：メッセージ シグナル割り込み（MSI） • **msix**：機能拡張されたメッセージ シグナル割り込み（MSI-X）。 これは推奨オプションであり、デフォルトになっています。
ステップ 24	Server /chassis/adapter/host-eth-if/interrupt # **exit**	ホスト イーサネット インターフェイス コマンド モードを終了します。
ステップ 25	Server /chassis/adapter/host-eth-if # **scope recv-queue**	受信キューのコマンド モードを開始します。
ステップ 26	Server /chassis/adapter/host-eth-if/recv-queue # **set rq-count** *count*	割り当てる受信キュー リソースの数。 指定できる値の範囲は、1～256です。デフォルトは、4 です。
ステップ 27	Server /chassis/adapter/host-eth-if/recv-queue # **set rq-ring-size** *size*	受信キュー内の記述子の数。 指定できる範囲は 64 ～ 4094 です。デフォルト値は 512 です。
ステップ 28	Server /chassis/adapter/host-eth-if/recv-queue # **exit**	ホスト イーサネット インターフェイス コマンド モードを終了します。

	コマンドまたはアクション	目的
ステップ 29	Server /chassis/adapter/host-eth-if # **scope trans-queue**	送信キューのコマンド モードを開始します。
ステップ 30	Server /chassis/adapter/host-eth-if/trans-queue # **set wq-count** *count*	割り当てる送信キュー リソースの数。 指定できる範囲は 1 ～ 256 です。デフォルト値は 1 です。
ステップ 31	Server /chassis/adapter/host-eth-if/trans-queue # **set wq-ring-size** *size*	送信キュー内の記述子の数。 指定できる範囲は 64 ～ 4094 です。デフォルト値は 256 です。
ステップ 32	Server /chassis/adapter/host-eth-if/trans-queue # **exit**	ホスト イーサネット インターフェイス コマンド モードを終了します。
ステップ 33	Server /chassis/adapter/host-eth-if # **scope comp-queue**	完了キューのコマンド モードを開始します。
ステップ 34	Server /chassis/adapter/host-eth-if/comp-queue # **set cq-count** *count*	割り当てる完了キュー リソースの数。 指定できる値の範囲は、1～512 です。デフォルトは、5 です。 一般に、完了キューの数は、送信キューの数と受信キューの数の合計と等しくなります。
ステップ 35	Server /chassis/adapter/host-eth-if/comp-queue # **exit**	ホスト イーサネット インターフェイス コマンド モードを終了します。
ステップ 36	Server /chassis/adapter/host-eth-if # **scope offload**	TCP オフロードのコマンド モードを開始します。
ステップ 37	Server /chassis/adapter/host-eth-if/offload # **set tcp-segment-offload** {**disable** | **enable**}	次のように、TCP セグメンテーション オフロードをイネーブルまたはディセーブルにします。 • **disable**：CPU は大きな TCP パケットをセグメント化します。 • **enable**：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。 これはデフォルトです。 （注） このオプションは、Large Send Offload（LSO）とも呼ばれています。

	コマンドまたはアクション	目的
ステップ 38	Server /chassis/adapter/host-eth-if/offload # **set tcp-rx-checksum-offload** {**disable** | **enable**}	次のように、TCP受信オフロードのチェックサム検証をイネーブルまたはディセーブルにします。 • **disable**：CPU はすべてのパケット チェックサムを検証します。 • **enable**：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。 これはデフォルトです。
ステップ 39	Server /chassis/adapter/host-eth-if/offload # **set tcp-tx-checksum-offload** {**disable** | **enable**}	次のように、TCP送信オフロードのチェックサム検証をイネーブルまたはディセーブルにします。 • **disable**：CPU はすべてのパケット チェックサムを検証します。 • **enable**：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。 これはデフォルトです。
ステップ 40	Server /chassis/adapter/host-eth-if/offload # **set tcp-large-receive-offload** {**disable** | **enable**}	次のように、TCP大きなパケット受信オフロードをイネーブルまたはディセーブルにします。 • **disable**：CPU はすべての大きなパケットを処理します。 • **enable**：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。 これはデフォルトです。
ステップ 41	Server /chassis/adapter/host-eth-if/offload # **exit**	ホスト イーサネット インターフェイス コマンド モードを終了します。
ステップ 42	Server /chassis/adapter/host-eth-if # **scope rss**	Receive Side Scaling（RSS）のコマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 43	Server /chassis/adapter/host-eth-if/rss # **set rss** {**disable** | **enable**}	マルチプロセッサ システム内でネットワーク受信処理の複数の CPU への効率的な配分を可能にする RSS をイネーブルまたはディセーブルにします。デフォルトでは、2 つのデフォルト vNIC に対してはイネーブル、ユーザ作成の vNIC に対してはディセーブルです。
ステップ 44	Server /chassis/adapter/host-eth-if/rss # **set rss-hash-ipv4** {**disable** | **enable**}	IPv4 RSS をイネーブルまたはディセーブルにします。 デフォルトはイネーブルです。
ステップ 45	Server /chassis/adapter/host-eth-if/rss # **set rss-hash-tcp-ipv4** {**disable** | **enable**}	TCP/IPv4 RSS をイネーブルまたはディセーブルにします。 デフォルトはイネーブルです。
ステップ 46	Server /chassis/adapter/host-eth-if/rss # **set rss-hash-ipv6** {**disable** | **enable**}	IPv6 RSS をイネーブルまたはディセーブルにします。 デフォルトはイネーブルです。
ステップ 47	Server /chassis/adapter/host-eth-if/rss # **set rss-hash-tcp-ipv6** {**disable** | **enable**}	TCP/IPv6 RSS をイネーブルまたはディセーブルにします。 デフォルトはイネーブルです。
ステップ 48	Server /chassis/adapter/host-eth-if/rss # **set rss-hash-ipv6-ex** {**disable** | **enable**}	IPv6 拡張 RSS をイネーブルまたはディセーブルにします。デフォルトはディセーブルです。
ステップ 49	Server /chassis/adapter/host-eth-if/rss # **set rss-hash-tcp-ipv6-ex** {**disable** | **enable**}	TCP/IPv6 拡張 RSS をイネーブルまたはディセーブルにします。 デフォルトはディセーブルです。
ステップ 50	Server /chassis/adapter/host-eth-if/rss # **exit**	ホスト イーサネット インターフェイス コマンド モードを終了します。
ステップ 51	Server /chassis/adapter/host-eth-if # **commit**	トランザクションをシステムの設定にコミットします。 （注） 変更した内容は、サーバを次にリブートしたときに有効になります。

次の例では、vNIC のプロパティを設定しています。

```
Server# scope chassis
Server /chassis # show adapter
PCI Slot Product Name   Serial Number  Product ID     Vendor
-------- -------------- -------------- -------------- --------------------
1        UCS VIC P81E   QCI1417A0QK    N2XX-ACPCI01   Cisco Systems Inc

Server /chassis # scope adapter 1
Server /chassis/adapter # scope host-eth-if Test1
Server /chassis/adapter/host-eth-if # set uplink 1
Server /chassis/adapter/host-eth-if *# scope offload
Server /chassis/adapter/host-eth-if/offload *# set tcp-segment-offload enable
Server /chassis/adapter/host-eth-if/offload *# exit
Server /chassis/adapter/host-eth-if *# commit
```

```
Server /chassis/adapter/host-eth-if #
```

次の作業

サーバをリブートして変更を適用します。

vNIC の作成

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

はじめる前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scope adapter** *index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンド モードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。
ステップ 3	Server /chassis/adapter # **create host-eth-if** *name*	vNIC を作成し、ホストのイーサネット インターフェイスのコマンド モードを開始します。 *name* 引数には最大 32 文字の ASCII 文字を使用できます。
ステップ 4	Server /chassis/adapter/host-eth-if # **set channel-number** *number*	（任意） アダプタで NIV モードがイネーブルになっている場合、この vNIC にチャネル番号を割り当てる必要があります。 指定できる範囲は 1 ～ 1000 です。
ステップ 5	Server /chassis/adapter/host-eth-if # **commit**	トランザクションをシステムの設定にコミットします。 （注） 変更した内容は、サーバを次にリブートしたときに有効になります。

次に、アダプタ 1 の vNIC を作成する例を示します。

```
Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # create host-eth-if Vnic5
Server /chassis/adapter/host-eth-if *# commit
New host-eth-if settings will take effect upon the next server reset
Server /chassis/adapter/host-eth-if #
```

vNIC の削除

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scope adapter** *index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンドモードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。
ステップ 3	Server /chassis/adapter # **delete host-eth-if** *name*	指定された vNIC を削除します。 （注） デフォルトの 2 つの vNIC（[eth0] と [eth1]）は、どちらも削除することはできません。
ステップ 4	Server /chassis/adapter # **commit**	トランザクションをシステムの設定にコミットします。 （注） 変更した内容は、サーバを次にリブートしたときに有効になります。

次に、アダプタ 1 の vNIC を削除する例を示します。

```
Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # delete host-eth-if Vnic5
Server /chassis/adapter *# commit
Server /chassis/adapter #
```

VM FEX の管理

仮想マシン ファブリック エクステンダ

Cisco Virtual Machine ファブリック エクステンダ（VM FEX）は、（prestandard）IEEE 802.1Qbh ポートエクステンダ アーキテクチャを仮想マシンにまで拡張します。このアーキテクチャでは、各 VM インターフェイスに対してスイッチ上で仮想 Peripheral Component Interconnect Express（PCIe）デバイスと仮想ポートが提供されます。

VM 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 カードがシャーシに装着され、サーバの電源がオンになっている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scope adapter** *index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンド モードを開始します。 （注） アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。
ステップ 3	Server /chassis/adapter # **show vmfex** [**detail**]	一般的な VM FEX プロパティを表示します。フィールドの説明については、全般的なプロパティ設定, （109 ページ）を参照してください。
ステップ 4	Server /chassis/adapter # **scope vmfex** *name*	指定された VM FEX インターフェイスのコマンド モードを開始します。
ステップ 5	Server /chassis/adapter/vmfex # **show interrupt** [**detail**]	イーサネット割り込み設定を表示します。 フィールドの説明については、イーサネット割り込みの設定, （110 ページ）を参照してください。
ステップ 6	Server /chassis/adapter/vmfex # **show recv-queue** [**detail**]	イーサネット受信キューの設定を表示します。フィールドの説明については、イーサネット受信キューの設定, （111 ページ）を参照してください。
ステップ 7	Server /chassis/adapter/vmfex # **show trans-queue** [**detail**]	イーサネット送信キューの設定を表示します。フィールドの説明については、イーサネット送信キューの設定, （111 ページ）を参照してください。
ステップ 8	Server /chassis/adapter/vmfex # **show comp-queue** [**detail**]	完了キューの設定を表示します。 フィールドの説明については、完了キューの設定, （111 ページ）を参照してください。

	コマンドまたはアクション	目的
ステップ 9	Server /chassis/adapter/vmfex # **show offload** [**detail**]	TCP オフロードの設定を表示します。 フィールドの説明については、TCP オフロードの設定, （111 ページ）を参照してください。
ステップ 10	Server /chassis/adapter/vmfex # **show rss** [**detail**]	RSS 設定を表示します。 フィールドの説明については、Receive Side Scaling 設定, （112 ページ）を参照してください。

次に、VM FEX のプロパティを表示する例を示します。

```
Server /chassis/adapter # show vmfex detail
Name pts0:
    MTU: 1500
    Uplink Port: 0
    MAC Address: 00:00:00:00:00:00
    CoS: N/A
    Trust Host CoS:
    PCI Order:
    VLAN: N/A
    VLAN Mode: N/A
    Rate Limiting:
    PXE Boot: disabled
    Channel Number: 0
    Port Profile:
    Uplink Failover: Enabled
    Uplink Failback Timeout: 5

Server /chassis/adapter # scope vmfex pts0

Server /chassis/adapter/vmfex # show interrupt
Interrupt Count Coalescing Time (us) Coalescing Type Interrupt Mode
--------------- -------------------- --------------- ---------------
6               125                  MIN             MSI

Server /chassis/adapter/vmfex # show recv-queue
Receive Queue Count Receive Queue Ring Size
------------------- ------------------------------
4                   512

Server /chassis/adapter/vmfex # show trans-queue
Transmit Queue Count Transmit Queue Ring Size
-------------------- -------------------------------
1                    256

Server /chassis/adapter/vmfex # show comp-queue
Completion Queue Count    Completion Queue Ring Size
------------------------- --------------------------
5                         1

Server /chassis/adapter/vmfex # show offload
TCP Segment Offload  TCP Rx Checksum  TCP Tx Checksum  Large Receive
-------------------- ---------------- ---------------- -------------
enabled              enabled          enabled          enabled

Server /chassis/adapter/vmfex # show rss
TCP Rx Side Scaling
--------------------
enabled

Server /chassis/adapter/vmfex #
```

VM FEX 設定

次の表に、表示できる VM FEX 設定について説明します。

全般的なプロパティ設定

名前	説明
Name	VM FEX のユーザ定義名。
MTU	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。
Uplink Port	この VM FEX に関連付けられたアップリンク ポート。 この VM FEX へのすべてのトラフィックは、このアップリンク ポートを通過します。
MAC Address	VM FEX に関連付けられた MAC アドレス。
Class of Service	この VM FEX からのトラフィックに関連付けられるサービス クラス。
Trust Host CoS	VM FEX がホスト オペレーティング システムが提供するサービス クラスを使用できるかどうか。
PCI Order	この VM FEX が使用される順序。
Default VLAN	この VM FEX のデフォルト VLAN。
VLAN Mode	VLAN トランキングまたはアクセスが設定されているかどうか。
Rate Limit	レート制限が設定されている場合、最大レート。
Enable PXE Boot	VM FEX を使用して PXE ブートを実行できるかどうか。
Channel Number	アダプタで NIV モードがイネーブルにされている場合、この VM FEX に割り当てられるチャネル番号。
Port Profile	アダプタで NIV モードがイネーブルにされている場合、VM FEX に関連付けられたポート プロファイル。 （注） このフィールドには、このサーバが接続しているスイッチに定義されたポート プロファイルが表示されます。

名前	説明
Enable Uplink Failover	アダプタでNIVモードがイネーブルにされている場合、通信に問題が発生したときにこのVM FEX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。
Failback Timeout	セカンダリ インターフェイスを使用してVM FEXが始動した後、そのVM FEX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。

イーサネット割り込みの設定

名前	説明
[Interrupt Count] フィールド	このVM FEXに割り当てられた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]：システムは、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。

イーサネット受信キューの設定

名前	説明
[Receive Queue Count] フィールド	この VM FEX に割り当てられた受信キュー 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。

イーサネット送信キューの設定

名前	説明
[Transmit Queue Count] フィールド	この VM FEX に割り当てられた送信キュー 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。

完了キューの設定

名前	説明
[Completion Queue Count] フィールド	この VM FEX に割り当てられた完了キュー 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。

TCP オフロードの設定

名前	説明
[Enable TCP Segmentation Offload] フィールド	イネーブルの場合、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。ディセーブルの場合、CPU は大きいパケットをセグメント化します。 （注） このオプションは、Large Send Offload（LSO）とも呼ばれています。
[Enable TCP Rx Offload Checksum Validation] フィールド	イネーブルの場合、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。ディセーブルの場合、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	イネーブルの場合、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。 ディセーブルの場合、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	イネーブルの場合、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。 ディセーブルの場合、CPU は大きいパケットをすべて処理します。

Receive Side Scaling 設定

名前	説明
[Enable TCP Receive Side Scaling] フィールド	Receive Side Scaling（RSS）は、ネットワーク受信処理をマルチプロセッサ システム内の複数の CPU に分散させます。 イネーブルの場合、可能であれば、ネットワーク受信処理がプロセッサ間で共有されます。ディセーブルの場合、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	イネーブルの場合、RSS が IPv4 ネットワークでイネーブルになります。
[Enable TCP-IPv4 RSS] フィールド	イネーブルの場合、IPv4 ネットワーク間での TCP 送信に対して RSS がイネーブルになります。
[Enable IPv6 RSS] フィールド	イネーブルの場合、RSS が IPv6 ネットワークでイネーブルになります。
[Enable TCP-IPv6 RSS] フィールド	イネーブルの場合、IPv6 ネットワーク間での TCP 送信に対して RSS がイネーブルになります。
[Enable IPv6 Extension RSS] フィールド	イネーブルの場合、IPv6 拡張に対して RSS がイネーブルになります。
[Enable TCP-IPv6 Extension RSS] フィールド	イネーブルの場合、IPv6 ネットワーク間での TCP 送信に対して RSS がイネーブルになります。

アダプタ設定のバックアップと復元

アダプタ設定のエクスポート

アダプタ設定は、XML ファイルとして TFTP サーバにエクスポートできます。

重要 ファームウェアまたは BIOS の更新が進行中の場合は、それらのタスクが完了するまで、アダプタ構成をエクスポートしないでください。

はじめる前に

Cisco UCS P81E 仮想インターフェイス カードがシャーシに装着され、サーバの電源がオンになっている必要があります。

TFTP サーバの IP アドレスを取得します。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scope adapter** *index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンド モードを開始します。 **（注）** アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。
ステップ 3	Server /chassis/adapter # **export-vnic** *tftp-ip-address path-and-filename*	エクスポート操作を開始します。アダプタ コンフィギュレーション ファイルは、指定した IP アドレスにある TFTP サーバ上に指定したパスとファイル名で保存されます。

次に、アダプタ 1 設定をエクスポートする例を示します。

```
Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # export-vnic 192.0.2.34 /ucs/backups/adapter4.dat
Server /chassis/adapter #
```

アダプタ設定のインポート

重要　ファームウェアまたは BIOS の更新が進行中の場合は、それらのタスクが完了するまで、アダプタ構成をインポートしないでください。

はじめる前に

このタスクを実行するには、admin 権限を持ってログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **scope adapter** *index*	*index* で指定した PCI スロット番号に装着されているアダプタ カードに対してコマンド モードを開始します。 （注）　アダプタの設定を表示または変更する前に、サーバの電源をオンにしておく必要があります。
ステップ 3	Server /chassis/adapter # **import-vnic** *tftp-ip-address path-and-filename*	インポート操作を開始します。 アダプタは、指定された IP アドレスの TFTP サーバから、指定されたパスの設定ファイルをダウンロードします。 この設定は、サーバが次にリブートされたときにインストールされます。

次に、PCI スロット 1 のアダプタの設定をインポートする例を示します。

```
Server# scope chassis
Server /chassis # scope adapter 1
Server /chassis/adapter # import-vnic 192.0.2.34 /ucs/backups/adapter4.xml
Import succeeded.
New VNIC adapter settings will take effect upon the next server reset.
Server /chassis/adapter #
```

次の作業

サーバをリブートして、インポートした設定を適用します。

アダプタのデフォルトの復元

はじめる前に

このタスクを実行するには、admin 権限を持ってログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis/adapter # **adapter-reset-defaults** *index*	*index* 引数で指定された PCI スロット番号のアダプタを出荷時の設定に復元します。 （注） 変更した内容は、サーバを次にリブートしたときに有効になります。

次に、PCI スロット 1 のアダプタのデフォルト設定を復元する例を示します。

```
Server# scope chassis
Server /chassis # adapter-reset-defaults 1
Factory default has been successfully restored.
Server /chassis #
```

次の作業

サーバをリブートして変更を適用します。

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。

アダプタ ファームウェアのインストール

重要 ファームウェアまたは BIOS の更新が進行中の場合は、それらのタスクが完了するまで、アダプタ ファームウェアをインストールしないでください。

はじめる前に

このタスクを実行するには、admin 権限を持ってログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **update-adapter-fw** *tftp-ip-address path-and-filename* {**activate** | **no-activate**} [*pci-slot*] [*pci-slot*]	指定したアダプタ ファームウェア ファイルを TFTP サーバからダウンロードし、アダプタを指定した場合は 1 つまたは 2 つの指定アダプタ上に、指定しなかった場合にはすべてのアダプタ上にこのファームウェアをバックアップイメージとしてインストールします。**activate** キーワードを指定した場合、新しいファームウェアがインストール後にアクティブになります。
ステップ 3	Server /chassis # **recover-adapter-update** [*pci-slot*] [*pci-slot*]	（任意） アダプタを指定した場合には 1 つまたは 2 つの指定アダプタについて、指定しない場合にはすべてのアダプタについて、不完全なファームウェア アップデートの状態をクリアします。

次に、PCI スロット 1 のアダプタ上のアダプタ ファームウェア アップグレードを開始する例を示します。

```
Server# scope chassis
Server /chassis # update-adapter-fw 192.0.2.34 /ucs/adapters/adapter4.bin activate 1
Server /chassis #
```

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, （117 ページ）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

重要　アクティブ化の進行中には、次のことを行わないでください。

- サーバのリセット、電源オフ、シャット ダウン。
- CIMC のリブートまたはリセット。
- 他のファームウェアのアクティブ化。
- テクニカル サポートまたは設定データのエクスポート。

はじめる前に

このタスクを実行するには、admin 権限を持ってログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope chassis**	シャーシ コマンド モードを開始します。
ステップ 2	Server /chassis # **activate-adapter-fw** *pci-slot* {**1** | **2**}	指定された PCI スロットのアダプタ上のアダプタ ファームウェア イメージ 1 または 2 をアクティブ化します。 （注）　変更した内容は、サーバを次にリブートしたときに有効になります。

次に、PCI スロット 1 のアダプタ上のアダプタ ファームウェア イメージ 2 をアクティブにする例を示します。

```
Server# scope chassis
Server /chassis # activate-adapter-fw 1 2
Firmware image activation suceeded
Please reset the server to run the activated image
Server /chassis #
```

次の作業

サーバをリブートして変更を適用します。

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，119 ページ
- SSH の設定，120 ページ
- XML API の設定，121 ページ
- IPMI の設定，122 ページ
- SNMP の設定，124 ページ

HTTP の設定

はじめる前に

HTTP 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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope http**	HTTP コマンド モードを開始します。
ステップ 2	Server /http # **set enabled** {**yes** | **no**}	CIMC で HTTP および HTTPS サービスをイネーブルまたはディセーブルにします。
ステップ 3	Server /http # **set http-port** *number*	HTTP 通信に使用するポートを設定します。 デフォルトは 80 です。
ステップ 4	Server /http # **set https-port** *number*	HTTPS 通信に使用するポートを設定します。 デフォルトは 443 です。

	コマンドまたはアクション	目的
ステップ 5	Server /http # **set http-redirect** {**yes** | **no**}	HTTPS への HTTP 要求のリダイレクトをイネーブルまたはディセーブルにします。
ステップ 6	Server /http # **set timeout** *seconds*	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を設定します。 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。
ステップ 7	Server /http # **commit**	トランザクションをシステムの設定にコミットします。

次に、CIMC に HTTP を設定する例を示します。

```
Server# scope http
Server /http # set enabled yes
Server /http *# set http-port 80
Server /http *# set https-port 443
Server /http *# set http-redirect yes
Server /http *# set timeout 1800
Server /http *# commit
Server /http # show
HTTP Port  HTTPS Port Timeout  Active Sessions Enabled HTTP Redirected
---------- ---------- -------- --------------- ------- ----------------
80         443        1800     0               yes     yes

Server /http #
```

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope ssh**	SSH コマンド モードを開始します。
ステップ 2	Server /ssh # **set enabled** {**yes** | **no**}	CIMC で SSH をイネーブルまたはディセーブルにします。
ステップ 3	Server /ssh # **set ssh-port** *number*	セキュア シェル アクセスに使用するポートを設定します。 デフォルトは 22 です。
ステップ 4	Server /ssh # **set timeout** *seconds*	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を設定します。

	コマンドまたはアクション	目的
		60 ～ 10,800 の範囲の整数を入力します。 デフォルトは 300 秒です。
ステップ 5	Server /ssh # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 6	Server /ssh # **show** [**detail**]	（任意）SSH の設定を表示します。

次に、CIMC に SSH を設定する例を示します。

```
Server# scope ssh
Server /ssh # set enabled yes
Server /ssh *# set ssh-port 22
Server /ssh *# set timeout 600
Server /ssh *# commit
Server /ssh # show
SSH Port   Timeout  Active Sessions Enabled
---------- -------- --------------- -------
22         600      1               yes

Server /ssh #
```

XML API の設定

CIMC 用の 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 サーバ用の CIMC に対するプログラマチック インターフェイスです。 この API は、HTTP または HTTPS 経由で XML ドキュメントを受け取ります。

XML API の詳細については、『*Cisco UCS Rack-Mount Servers 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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope xmlapi**	XML API コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	Server /xmlapi # **set enabled** {**yes** | **no**}	CIMC の XML API 制御をイネーブルまたはディセーブルにします。
ステップ 3	Server /xmlapi # **commit**	トランザクションをシステムの設定にコミットします。

次に、CIMC の XML API 制御を有効にし、トランザクションをコミットする例を示します。

```
Server# scope xmlapi
Server /xmlapi # set enabled yes
Server /xmlapi *# commit
Server /xmlapi #  show detail
XMLAPI Settings:
    Enabled: yes
    Active Sessions: 0
    Max Sessions: 4

Server /xmlapi #
```

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 権限を持ってログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope ipmi**	IPMI コマンド モードを開始します。
ステップ 2	Server /ipmi # **set enabled** {**yes** | **no**}	このサーバで IPMI アクセスをイネーブルまたはディセーブルにします。
ステップ 3	Server /ipmi # **set privilege-level** {**readonly** | **user** | **admin**}	このサーバで IPMI セッションに割り当て可能な最高特権レベルを指定します。ここに表示される値は次のとおりです。 • **readonly**：IPMI ユーザは情報を表示できますが、変更できません。 このオプションを選択した場合、「Administrator」、「Operator」、または「User」ユーザ ロールを持つ IPMI ユーザが作成できるのは、読み取り専用の IPMI セッションだけです。それ以外に所持している IPMI 特権は関係ありません。 • **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した場合、「Administrator」または「Operator」ユーザ ロールを持つ IPMI ユーザがこのサーバで作成できるのは、ユーザ セッションと読み取り専用セッションだけです。 • **admin**：IPMI ユーザは使用可能なすべてのアクションを実行できます。 このオプションを選択した場合、「Administrator」ユーザ ロールを持つ IPMI ユーザは、管理者、ユーザ、および読み取り専用セッションをこのサーバで作成できます。
ステップ 4	Server /ipmi # **set encryption-key** *key*	IPMI 通信に使用する IPMI 暗号キーを設定します。 キーの値は、40 個の 16 進数であることが必要です。
ステップ 5	Server /ipmi # **commit**	トランザクションをシステムの設定にコミットします。

次に、CIMC に IPMI over LAN を設定する例を示します。

```
Server# scope ipmi
Server /ipmi # set enabled yes
Server /ipmi *# set privilege-level admin
Server /ipmi *# set encryption-key abcdef01234567890abcdef01234567890abcdef
Server /ipmi *# commit
Server /ipmi # show
Enabled Encryption Key                          Privilege Level Limit
------- --------------------------------------- ---------------------
yes     abcdef01234567890abcdef01234567890abcdef admin

Server /ipmi #
```

SNMP の設定

SNMP

Cisco UCS C シリーズ ラックマウント サーバ は、サーバの設定およびステータスを表示したり、SNMP トラップによって障害とアラートを送信したりするために、簡易ネットワーク管理プロトコル（SNMP）をサポートしています。 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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope snmp**	SNMP コマンド モードを開始します。
ステップ 2	Server /snmp # **set enabled** {**yes** | **no**}	SNMP をイネーブルまたはディセーブルにします。 （注） 追加の SNMP コンフィギュレーション コマンドが受け入れられる前には、SNMP をイネーブルにして保存する必要があります。
ステップ 3	Server /snmp # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 4	Server /snmp # **set community-str** *community*	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 コミュニティ名を指定します。 名前には最大 18 文字を使用できます。
ステップ 5	Server /snmp # **set sys-contact** *contact*	SNMP の実装を担当する、システムの連絡先を指定します。 連絡先情報には、電子メールアドレス、名前と電話番号などを最大 254 文字で指定できます。 スペースが含まれている値を入力するには、エントリを引用符で囲む必要があります。
ステップ 6	Server /snmp # **set sys-location** *location*	SNMP エージェント（サーバ）が実行されるホストの場所を指定します。 ロケーション情報には最大 254 文

	コマンドまたはアクション	目的
		字を使用できます。スペースが含まれている値を入力するには、エントリを引用符で囲む必要があります。
ステップ 7	Server /snmp # **commit**	トランザクションをシステムの設定にコミットします。

次に、SNMP プロパティを設定し、トランザクションをコミットする例を示します。

```
Server# scope snmp
Server /snmp # set enabled yes
Server /snmp *# commit
Server /snmp # set community-str cimcpublic
Server /snmp *# set sys-contact "User Name <username@example.com> +1-408-555-1212"
Server /snmp *# set sys-location "San Jose, California"
Server /snmp *# commit
Server /snmp #  show detail
SNMP Settings:
    SNMP Port: 161
    System Contact: User Name <username@example.com> +1-408-555-1212
    System Location: San Jose, California
    SNMP Community: cimcpublic
    SNMP Trap community: 0
    Enabled: yes
    SNMP Trap Version: 1
    SNMP Inform Type: inform

Server /snmp #
```

次の作業

「SNMP トラップ設定の指定, （125 ページ）」の説明に従って SNMP トラップ設定を設定します。

SNMP トラップ設定の指定

はじめる前に

- このタスクを実行するには、admin 権限を持ってログインする必要があります。
- トラップの設定を実行する前に、SNMP をイネーブルにして保存する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope snmp**	SNMP コマンド モードを開始します。
ステップ 2	Server /snmp # **set trap-community-str** *string*	トラップ情報の送信先となる SNMP コミュニティの名前を入力します。

	コマンドまたはアクション	目的
ステップ 3	Server /snmp # **set trap-ver** {**1** | **2** | **3**}	必要なトラップ メッセージの SNMP バージョンを指定します。 （注） SNMPv3 トラップは SNMPv3 ユーザおよびキー値が正しく設定されている場所だけに配信されます。
ステップ 4	Server /snmp # **set inform-type** {**trap** | **inform**}	SNMP 通知メッセージを単純なトラップとして送信するのか、レシーバによる確認応答が必要なインフォーム要求として送信するかを指定します。
ステップ 5	Server /snmp # **scope trap-destination** *number*	指定した宛先に対して SNMP トラップ宛先コマンド モードを開始します。 4 つの SNMP トラップ宛先を使用できます。 宛先の *number* は、1 ～ 4 の範囲の整数です。
ステップ 6	Server /snmp/trap-destination # **set enabled** {**yes** | **no**}	SNMP トラップ宛先をイネーブルまたはディセーブルにします。
ステップ 7	Server /snmp/trap-destination # **set addr** *ip-address*	SNMP トラップ情報を送信する宛先 IP アドレスを指定します。
ステップ 8	Server /snmp/trap-destination # **commit**	トランザクションをシステムの設定にコミットします。

次に、汎用の SNMP トラップとトラップの宛先番号 1 を設定し、トランザクションをコミットする例を示します。

```
Server# scope snmp
Server /snmp # set trap-community-str public
Server /snmp # set trap-ver 3
Server /snmp # set inform-type inform
Server /snmp *# scope trap-destination 1
Server /snmp/trap-destination *# set enabled yes
Server /snmp/trap-destination *# set addr 192.0.20.41
Server /snmp/trap-destination *# commit
Server /snmp/trap-destination # show
Trap Destination IP Address       Enabled
---------------- ---------------- --------
1                192.0.20.41      yes

Server /snmp/trap-destination #
```

テスト SNMP トラップ メッセージの送信

はじめる前に

このタスクを実行するには、admin 権限を持ってログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope snmp**	SNMP コマンド モードを開始します。
ステップ 2	Server /snmp # **scope trap-destination** *number*	指定した宛先に対して SNMP トラップ宛先コマンド モードを開始します。 4 つの SNMP トラップ宛先を使用できます。 宛先の *number* は、1 ～ 4 の範囲の整数です。
ステップ 3	Server /snmp/trap-destination # **sendSNMPtrap**	設定済みの SNMP トラップ宛先に SNMPv1 テスト トラップを送信します。 （注） テスト メッセージを送信するために、トラップは設定済みで、イネーブルにされている必要があります。

次の例では、SNMP トラップ宛先 1 にテスト メッセージが送信されます。

```
Server# scope snmp
Server /snmp # scope trap-destination 1
Server /snmp/trap-destination # sendSNMPtrap
SNMP Test Trap sent to Destination:1
Server /snmp/trap-destination #
```

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。
- これらのコンフィギュレーション コマンドが受け入れられる前には、SNMP をイネーブルにして保存する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope snmp**	SNMP コマンド モードを開始します。
ステップ 2	Server /snmp # **scope v3users** *number*	指定したユーザ番号の SNMPv3 ユーザのコマンド モードを開始します。
ステップ 3	Server /snmp/v3users # **set v3add** {**yes** | **no**}	SNMPv3 ユーザを追加または削除します。 次のいずれかになります。

	コマンドまたはアクション	目的
		• **yes**：このユーザは SNMPv3 ユーザとしてイネーブルであり、SNMP OID ツリーにアクセスできます。 （注） セキュリティ名とセキュリティ レベルがこの時点で設定されていないと、ユーザの追加に失敗します。 • **no**：このユーザ コンフィギュレーションは削除されます。
ステップ 4	Server /snmp/v3users # **set v3security-name** *security-name*	このユーザの SNMP ユーザ名を入力します。
ステップ 5	Server /snmp/v3users # **set v3security-level** {**noauthnopriv** | **authnopriv** | **authpriv**}	このユーザのセキュリティ レベルを選択します。次のいずれかになります。 • **noauthnopriv**：ユーザは許可またはプライバシー パスワードを必要としません。 • **authnopriv**：ユーザは許可パスワードを必要としますが、プライバシー パスワードは必要としません。 このオプションを選択した場合は、認証キーを設定する必要があります。 • **authpriv**：ユーザ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した場合は、認証キーおよび秘密暗号キーを設定する必要があります。
ステップ 6	Server /snmp/v3users # **set v3proto** {**MD5** | **SHA**}	このユーザの認証プロトコルを選択します。
ステップ 7	Server /snmp/v3users # **set v3auth-key** *auth-key*	このユーザの許可パスワードを入力します。
ステップ 8	Server /snmp/v3users # **set v3priv-proto** {**DES** | **AES**}	このユーザの暗号化プロトコルを選択します。
ステップ 9	Server /snmp/v3users # **set v3priv-auth-key** *priv-auth-key*	このユーザの秘密暗号キー（プライバシーパスワード）を入力します。
ステップ 10	Server /snmp/v3users # **commit**	トランザクションをシステムの設定にコミットします。

次に、SNMPv3 ユーザ番号 2 を設定し、トランザクションをコミットする例を示します。

```
Server# scope snmp
Server /snmp # scope v3users 2
```

```
Server /snmp/v3users # set v3add yes
Server /snmp/v3users *# set v3security-name ucsSNMPV3user
Server /snmp/v3users *# set v3security-level authpriv
Server /snmp/v3users *# set v3proto SHA
Server /snmp/v3users *# set v3auth-key
Please enter v3auth-key:ex4mp1ek3y
Please confirm v3auth-key:ex4mp1ek3y
Server /snmp/v3users *# set v3priv-proto AES
Server /snmp/v3users *# set v3priv-auth-key
Please enter v3priv-auth-key:!1@2#3$4%5^6&7*8
Please confirm v3priv-auth-key:!1@2#3$4%5^6&7*8
Server /snmp/v3users *# commit
Settings are being applied ... allow a few minutes for the process to complete
Server /snmp/v3users # show detail
User 2:
    Add User: yes
    Security Name: ucsSNMPV3user
    Security Level: authpriv
    Auth Type: SHA
    Auth Key: ******
    Encryption: AES
    Private Key: ******

Server /snmp/v3users #
```

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，131 ページ
- 証明書署名要求の生成，132 ページ
- 自己署名証明書の作成，133 ページ
- サーバ証明書のアップロード，136 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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope certificate**	証明書コマンド モードを開始します。
ステップ 2	Server /certificate # **generate-csr**	Certificate Signing Request（CSR; 証明書署名要求）の生成に関するダイアログを起動します。

証明書署名要求に関して、次の情報の入力を求めるプロンプトが表示されます。

Common Name（CN）	CIMC の完全修飾ホスト名
Organization Name (O)	証明書を要求している組織。
Organization Unit (OU)	組織ユニット
Locality（L）	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。
StateName (S)	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 (CC)	会社の本社が存在する国を示す 2 文字の ISO 国コード。
Email	会社の管理用電子メールの連絡先。

要求された情報を入力すると、証明書署名要求が生成され、コンソール出力に表示されます。CSR ファイルは作成されませんが、コンソール出力から CSR 情報をコピーして、テキストファイルに貼り付けることができます。

次に、証明書署名要求を生成する例を示します。

```
Server# scope certificate
Server /certificate # generate-csr
Common Name (CN): test.example.com
Organization Name (O): Example, Inc.
Organization Unit (OU): Test Department
```

```
Locality (L): San Jose
StateName (S): CA
Country Code (CC): US
Email: user@example.com
Continue to generate CSR?[y|N]y


-----BEGIN CERTIFICATE REQUEST-----
MIIB/zCCAWgCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGA1UE
BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
ZgAMivyCsKgb/6CjQtsofvzxmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKONDl
GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
-----END CERTIFICATE REQUEST-----

Copy everything from "-----BEGIN ..."  to "END CERTIFICATE REQUEST-----",
paste to a file, send to your chosen CA for signing,
and finally upload the signed certificate via upload command.
            ---OR---
Continue to self sign CSR and overwrite the current certificate?
All HTTPS and SSH sessions will be disconnected. [y|N]N
```

次の作業

次のいずれかの作業を実行します。

- 公共の認証局から証明書を取得したくない場合に、組織が独自の認証局を運用していなければ、CSR から自己署名証明書を内部生成し、すぐにサーバにアップロードするよう、CIMC を設定できます。 この処理を行うには、この例では最後のプロンプトの後に **y** と入力します。
- 組織が自己署名証明書を生成するための独自の証明書サーバを運用している場合は、「-----BEGIN ...」から「END CERTIFICATE REQUEST-----」までのコマンド出力をコピーして、csr.txt というファイルに貼り付けます。 CSR ファイルを証明書サーバに入力して、自己署名証明書を生成します。
- 公共の認証局から証明書を取得する場合は、「-----BEGIN ...」から「END CERTIFICATE REQUEST-----」までのコマンド出力をコピーして、csr.txt というファイルに貼り付けます。 CSR ファイルを認証局に提出して、署名付き証明書を取得します。

CIMC によって自己署名証明書を内部生成し、アップロードする最初のオプションを使用しない場合は、証明書コマンドモードで **upload** コマンドを使用して新しい証明書をアップロードする必要があります。

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 設定ファイルに追加します。 この指定により、認証されたクライアントがサーバになりすます man-in-the-middle 攻撃を防御できます。 OpenSSL 設定ファイル openssl.conf には、"nsCertType＝server" という文が含まれています。
ステップ 4	**openssl x509 -req -days** *numdays* **-in** *CSR_filename* **-CA** *CA_certfilename* **-set_serial 04 -CAkey** *CA_keyfilename* **-out** *server_certfilename* **-extfile openssl.conf**	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。

	コマンドまたはアクション	目的
	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は、読み取り可能テキストとして使用できる必要があります。 アップロード手順で、証明書テキストをコピーして CLI に貼り付けます。

（注） 最初に、CIMC 証明書管理 CSR の生成手順を使用して CSR を生成し、その CSR を使用してアップロード用の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。

（注） 新しいサーバ証明書がアップロードされると、現在の HTTPS および SSH セッションはすべて切断されます。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope certificate**	証明書コマンド モードを開始します。
ステップ 2	Server /certificate # **upload**	新しいサーバ証明書を入力してアップロードするためのダイアログが起動します。

プロンプトが表示されたら、証明書テキストをコピーしてコンソールに貼り付け、CTRL を押した状態で D を押して証明書をアップロードします。

次に、新しい証明書をサーバにアップロードする例を示します。

```
Server# scope certificate
Server /certificate # upload
Please paste your certificate here, when finished, press CTRL+D.
-----BEGIN CERTIFICATE-----
MIIB/zCCAWgCAQAwgZkxCzAJBgNVBAYTAlVTMQswCQYDVQQIEwJDQTEVMBMGA1UE
BxMMU2FuIEpvc2UsIENBMRUwEwYDVQQKEwxFeGFtcGxlIEluYy4xEzARBgNVBAsT
ClRlc3QgR3JvdXAxGTAXBgNVBAMTEHRlc3QuZXhhbXBsZS5jb20xHzAdBgkqhkiG
9w0BCQEWEHVzZXJAZXhhbXBsZS5jb20wgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ
AoGBAMZw4nTepNIDhVzb0j7Z2Je4xAG56zmSHRMQeOGHemdh66u2/XAoLx7YCcYU
ZgAMivyCsKgb/6CjQtsofvzxmC/eAehuK3/SINv7wd6Vv2pBt6ZpXgD4VBNKOND1
GMbkPayVlQjbG4MD2dx2+H8EH3LMtdZrgKvPxPTE+bF5wZVNAgMBAAGgJTAjBgkq
hkiG9w0BCQcxFhMUQSBjaGFsbGVuZ2UgcGFzc3dvcmQwDQYJKoZIhvcNAQEFBQAD
gYEAG61CaJoJaVMhzCl903O6Mg51zq1zXcz75+VFj2I6rH9asckCld3mkOVx5gJU
Ptt5CVQpNgNLdvbDPSsXretysOhqHmp9+CLv8FDuy1CDYfuaLtvlWvfhevskV0j6
mK3Ku+YiORnv6DhxrOoqau8r/hyI/L43l7IPN1HhOi3oha4=
-----END CERTIFICATE-----
<CTRL+D>
```

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，137 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，138 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，138 ページ
- プラットフォーム イベント フィルタの設定，139 ページ
- SNMP トラップ設定の指定，141 ページ
- テスト SNMP トラップ メッセージの送信，142 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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope fault**	障害コマンド モードを開始します。
ステップ 2	Server /fault # **set platform-event-enabled yes**	プラットフォーム イベント アラートをイネーブルにします。
ステップ 3	Server /fault # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 4	Server /fault # **show** [**detail**]	（任意）プラットフォーム イベント アラートの設定を表示します。

次に、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例を示します。

```
Server# scope fault
Server /fault # set platform-event-enabled yes
Server /fault *# commit
Server /fault # show
SNMP Community String Platform Event Enabled
--------------------- ----------------------
public                yes

Server /fault #
```

プラットフォーム イベント アラートのディセーブル化

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope fault**	障害コマンド モードを開始します。
ステップ 2	Server /fault # **set platform-event-enabled no**	プラットフォーム イベント アラートをディセーブルにします。
ステップ 3	Server /fault # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 4	Server /fault # **show** [**detail**]	（任意）プラットフォーム イベント アラートの設定を表示します。

プラットフォーム イベント フィルタの設定

次に、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例を示します。

```
Server# scope fault
Server /fault # set platform-event-enabled no
Server /fault *# commit
Server /fault # show
SNMP Community String Platform Event Enabled
--------------------- ------------------------
public                no

Server /fault #
```

プラットフォーム イベント フィルタの設定

次のプラットフォーム イベント フィルタに対する処理とアラートを設定できます。

ID	プラットフォーム イベント フィルタ
1	温度緊急アサート フィルタ
2	温度警告アサート フィルタ
3	電圧緊急アサート フィルタ
4	電流アサート フィルタ
5	ファン緊急アサート フィルタ
6	プロセッサ アサート フィルタ
7	電源緊急アサート フィルタ
8	電源警告アサート フィルタ
9	電源冗長性損失フィルタ
10	ディスクリート電源アサート フィルタ
11	メモリ アサート フィルタ
12	ドライブ スロット アサート フィルタ

プラットフォーム イベント フィルタの設定

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope fault**	障害コマンド モードを開始します。
ステップ 2	Server /fault # **scope pef** *id*	指定したイベントに対してプラットフォーム イベント フィルタ コマンド モードを開始します。 イベント ID 番号に対応するプラットフォーム イベント フィルタの表を参照してください。
ステップ 3	Server /fault/pef # **set action** {**none** | **reboot** | **power-cycle** | **power-off**}	このイベントが発生した場合に必要なシステムの処理を選択します。 次のいずれかの処理を選択できます。 • **none**：システム アクションは実行されません。 • **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。
ステップ 4	Server /fault/pef # **set send-alert** {**yes** | **no**}	このイベントに対するプラットフォーム イベント アラートの送信をイネーブルまたはディセーブルにします。 （注） 送信するアラートについて、フィルタ トラップを正しく設定し、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必要があります。
ステップ 5	Server /fault/pef # **commit**	トランザクションをシステムの設定にコミットします。

次に、イベントに対するプラットフォーム イベント アラートを設定します。

```
Server# scope fault
Server /fault # scope pef 13
Server /fault/pef # set action reboot
Server /fault/pef *# set send-alert yes
Server /fault/pef *# commit
Server /fault/pef # show
Platform Event Filter Event                          Action      Send Alert
--------------------- ---------------------------- ----------- ------------------
13                    Memory Assert Filter         reboot      yes

Server /fault/pef #
```

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

- SNMP トラップ設定の実行

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 権限を持ってログインする必要があります。
- トラップの設定を実行する前に、SNMP をイネーブルにして保存する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope snmp**	SNMP コマンド モードを開始します。
ステップ 2	Server /snmp # **set trap-community-str** *string*	トラップ情報の送信先となる SNMP コミュニティの名前を入力します。
ステップ 3	Server /snmp # **set trap-ver** {**1** | **2** | **3**}	必要なトラップ メッセージの SNMP バージョンを指定します。 （注） SNMPv3 トラップは SNMPv3 ユーザおよびキー値が正しく設定されている場所だけに配信されます。
ステップ 4	Server /snmp # **set inform-type** {**trap** | **inform**}	SNMP 通知メッセージを単純なトラップとして送信するのか、レシーバによる確認応答が必要なインフォーム要求として送信するかを指定します。
ステップ 5	Server /snmp # **scope trap-destination** *number*	指定した宛先に対して SNMP トラップ宛先コマンド モードを開始します。 4 つの SNMP トラップ宛先を使用できます。 宛先の *number* は、1 ～ 4 の範囲の整数です。
ステップ 6	Server /snmp/trap-destination # **set enabled** {**yes** | **no**}	SNMP トラップ宛先をイネーブルまたはディセーブルにします。
ステップ 7	Server /snmp/trap-destination # **set addr** *ip-address*	SNMP トラップ情報を送信する宛先 IP アドレスを指定します。
ステップ 8	Server /snmp/trap-destination # **commit**	トランザクションをシステムの設定にコミットします。

次に、汎用の SNMP トラップとトラップの宛先番号 1 を設定し、トランザクションをコミットする例を示します。

```
Server# scope snmp
Server /snmp # set trap-community-str public
Server /snmp # set trap-ver 3
Server /snmp # set inform-type inform
Server /snmp *# scope trap-destination 1
Server /snmp/trap-destination *# set enabled yes
Server /snmp/trap-destination *# set addr 192.0.20.41
Server /snmp/trap-destination *# commit
Server /snmp/trap-destination # show
Trap Destination IP Address       Enabled
---------------- ---------------- --------
1                192.0.20.41      yes

Server /snmp/trap-destination #
```

テスト SNMP トラップ メッセージの送信

はじめる前に

このタスクを実行するには、admin 権限を持ってログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope snmp**	SNMP コマンド モードを開始します。
ステップ 2	Server /snmp # **scope trap-destination** *number*	指定した宛先に対して SNMP トラップ宛先コマンド モードを開始します。 4 つの SNMP トラップ宛先を使用できます。 宛先の *number* は、1 ～ 4 の範囲の整数です。
ステップ 3	Server /snmp/trap-destination # **sendSNMPtrap**	設定済みの SNMP トラップ宛先に SNMPv1 テスト トラップを送信します。 （注） テスト メッセージを送信するために、トラップは設定済みで、イネーブルにされている必要があります。

次の例では、SNMP トラップ宛先 1 にテスト メッセージが送信されます。

```
Server# scope snmp
Server /snmp # scope trap-destination 1
Server /snmp/trap-destination # sendSNMPtrap
SNMP Test Trap sent to Destination:1
Server /snmp/trap-destination #
```

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た 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` の形式で含まれています。 OID の最初の 10 個のフィールドは、
`iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).wired_for_management(3183).PET(1).version(1).version(0)`
を表し、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 メッセージであることを示しています。 最後のフィールドはイベント番号であり、通知されている特定の状態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

次の表に、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を示します。これらは、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	温度に関する警告
65801	010109h	温度が重大な状態
131330	020102h	電圧不足、緊急
131337	020109h	電圧が重大な状態
196871	030107h	電流に関する警告
262402	040102h	ファンが重大な状態
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	電源が重大な状態
524551	080107h	電源に関する警告
525313	080401h	個々の電源に関する警告
527105	080B01h	電源冗長性の損失
527106	080B02h	電源冗長性復元
552704	086F00h	電源挿入済み

イベント番号 [注記 1]		プラットフォーム イベントの説明
552705	086F01h	電源モジュール障害
552707	086F03h	電源 AC の損失
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
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 あり、障害の兆候なし
880385	0D6F01h	HDD の障害
880512	0D6F80h	HDD が存在しない
880513	0D6F81h	HDD がアサート解除された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

イベント番号 [注記 1]		プラットフォーム イベントの説明
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
- インストールした CIMC ファームウェアのアクティブ化，150 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，151 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。

（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。

インストールするもの

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することができます。
- 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。

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

シスコから CIMC ファームウェアを取得し、そのファイルをローカル TFTP サーバに保存します。

（注） アップデートがすでに処理中であるときにアップデートを開始すると、どちらのアップデートも失敗します。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope firmware**	CIMC ファームウェア コマンド モードを開始します。
ステップ 3	Server /cimc/firmware # **update** *tftp-ip-address path-and-filename*	ファームウェアのアップデートを開始します。サーバは、指定の IP アドレスにある TFTP サーバから、指定のパスとファイル名のアップデート ファームウェアを取得します。
ステップ 4	（任意）Server /cimc/firmware # **show detail**	ファームウェア アップデートの進捗状況を表示します。

次に、CIMC ファームウェアをアップデートする例を示します。

```
Server# scope cimc
Server /cimc # scope firmware
Server /cimc/firmware # update 192.0.20.34 //test/dnld-ucs-k9-bundle.1.0.2h.bin
  <CR>  Press Enter key
Firmware update has started.
Please check the status using "show detail"
Server /cimc/firmware #
```

次の作業

新しいファームウェアをアクティブにします。

インストールした CIMC ファームウェアのアクティブ化

はじめる前に

CIMC ファームウェアをサーバにインストールします。

（注） アップデートの処理中にアクティブ化を開始すると、アクティブ化に失敗します。

重要　アクティブ化の進行中には、次のことを行わないでください。

- サーバのリセット、電源オフ、シャット ダウン。
- CIMC のリブートまたはリセット。
- 他のファームウェアのアクティブ化。
- テクニカル サポートまたは設定データのエクスポート。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope firmware**	ファームウェア コマンドモードを開始します。
ステップ 3	Server /cimc/firmware # **show [detail]**	使用可能なファームウェア イメージおよびステータスを表示します。
ステップ 4	Server /cimc/firmware # **activate [1 | 2]**	選択したイメージをアクティブにします。 イメージ番号が指定されていない場合、サーバは現在非アクティブのイメージをアクティブにします。

次に、ファームウェア イメージ 1 をアクティブにする例を示します。

```
Server# scope cimc
Server /cimc # scope firmware
Server /cimc/firmware # show detail
Firmware Image Information:
    Update Stage: NONE
    Update Progress: 100
    Current FW Version: 1.0(0.74)
    FW Image 1 Version: 1.0(0.66a)
    FW Image 1 State: BACKUP INACTIVATED
    FW Image 2 Version: 1.0(0.74)
    FW Image 2 State: RUNNING ACTIVATED

Server /cimc/firmware # activate 1
```

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

シスコから BIOS ファームウェアを取得し、そのファイルをローカル TFTP サーバに保存します。

（注） アップデートがすでに処理中であるときにアップデートを開始すると、どちらのアップデートも失敗します。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope bios**	BIOS コマンド モードを開始します。
ステップ 2	Server /bios # **update** *tftp-ip-address path-and-filename*	BIOS ファームウェアのアップデートを開始します。 サーバは、指定の IP アドレスにある TFTP サーバから、指定のパスとファイル名のアップデート ファームウェアを取得します。

次に、BIOS ファームウェアをアップデートする例を示します。

```
Server# scope bios
Server /bios # update 192.0.20.34 //test/C240M3.1.4.4c.0.bin
  <CR>  Press Enter key
```

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, 153 ページ
- System Event Log, 157 ページ

CIMC ログ

CIMC ログの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope log**	CIMC ログ コマンド モードを開始します。
ステップ 3	Server /cimc/log # **show entries** [**detail**]	CIMC イベントをタイムスタンプ、イベントを記録したソフトウェア モジュール、およびイベントの説明とともに表示します。

次に、CIMC イベントのログを表示する例を示します。

```
Server# scope cimc
Server /cimc # scope log
Server /cimc/log # show entries
Time                 Severity      Source           Description

-------------------- ------------- ---------------- ----------------------------------------

2012 Jan 30 05:20:45 Informational BMC:ciscoNET:961 " rpc_aim_callback_function_1_svc() -
result == SUCCESS, callbackData size: 600 "
```

```
2012 Jan 30 05:20:45 Informational BMC:ciscoNET:961 rpc_aim_callback_function_1_svc() -
returned from pFunctionCallback result:0
2012 Jan 30 05:20:45 Informational BMC:ciscoNET:961 " rpc_aim_callback_function_1_svc() -
szFunctionName:netGetCurrentIfConfig nSize:0 nMaxSize: 600 "
--More--

Server /cimc/log # show entries detail
Trace Log:
    Time: 2012 Jan 30 05:20:45
    Severity: Informational
    Source: BMC:ciscoNET:961
   Description: " rpc_aim_callback_function_1_svc() - result == SUCCESS, callbackData size:
 600 "
    Order: 0
Trace Log:
    Time: 2012 Jan 30 05:20:45
    Severity: Informational
    Source: BMC:ciscoNET:961
   Description: rpc_aim_callback_function_1_svc() - returned from pFunctionCallback result:0

    Order: 1
Trace Log:
    Time: 2012 Jan 30 05:20:45
    Severity: Informational
    Source: BMC:ciscoNET:961
   Description: " rpc_aim_callback_function_1_svc() - szFunctionName:netGetCurrentIfConfig
 nSize:0 nMaxSize: 600 "
    Order: 2
--More--

Server /cimc/log #
```

CIMC ログのクリア

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope log**	CIMC ログ コマンド モードを開始します。
ステップ 3	Server /cimc/log # **clear**	CIMC ログをクリアします。

次に、CIMC イベントのログをクリアする例を示します。

```
Server# scope cimc
Server /cimc # scope log
Server /cimc/log # clear
```

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

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope log**	CIMC ログ コマンド モードを開始します。
ステップ 3	Server /cimc/log # **set local-syslog-severity** *level*	重大度の *level* には、次のいずれかを指定できます。順に重大度が下がります。 • 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。
ステップ 4	Server /cimc/log # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 5	Server /cimc/log # **show local-syslog-severity**	（任意） 設定された重大度レベルを表示します。

次に、最小重大度を警告として、メッセージのロギングを設定する例を示します。

```
Server# scope cimc
Server /cimc # scope log
Server /cimc/log # set local-syslog-severity warning
Server /cimc/log *# commit
Server /cimc/log # show local-syslog-severity
    Local Syslog Severity: warning

Server /cimc/log #
```

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 サーバが CIMC ログ エントリを受信するように、プロファイルを設定できます。

はじめる前に

- リモート syslog サーバは、リモート ホストからログを受信するように設定する必要があります。
- リモート syslog サーバは、認証関連のログを含むすべての種類のログを受信するように設定する必要があります。
- リモート syslog サーバのファイアウォールは、syslog メッセージが syslog サーバに到達できるよう設定する必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope log**	CIMC ログ コマンド モードを開始します。
ステップ 3	Server /cimc/log # **set remote-syslog-severity** *level*	（任意） 重大度の *level* には、次のいずれかを指定できます。順に重大度が下がります。 • 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、リモート Syslog サーバは重大度が Emergency、Alert、Critical、または Error の CIMC ログ メッセージすべてを受信します。 Warning、Notice、Informational、または Debug のメッセージは表示されません。

	コマンドまたはアクション	目的
ステップ 4	Server /cimc/log # **scope server** {**1** | **2**}	2 台のリモート Syslog サーバ プロファイルのいずれかを選択し、プロファイルを設定するコマンドモードを開始します。
ステップ 5	Server /cimc/log/server # **set server-ip** *ip-address*	リモート syslog サーバの IP アドレスを指定します。
ステップ 6	Server /cimc/log/server # **set enabled** {**yes** | **no**}	この syslog サーバへの CIMC ログ エントリの送信をイネーブルにします。
ステップ 7	Server /cimc/log/server # **commit**	トランザクションをシステムの設定にコミットします。

次に、リモート syslog サーバ プロファイルを設定し、重大度レベル Warning 以上の CIMC ログ エントリの送信をイネーブルにする例を示します。

```
Server# scope cimc
Server /cimc # scope log
Server /cimc/log # set remote-syslog-severity warning
Server /cimc/log *# scope server 2
Server /cimc/log/server *# set server-ip 192.0.2.34
Server /cimc/log/server *# set enabled yes
Server /cimc/log/server *# commit
Server /cimc/log/server # exit
Server /cimc/log # show server
Syslog Server    IP Address       Enabled
---------------- ---------------- --------
1                0.0.0.0          no
2                192.0.2.34       yes

Server /cimc/log # show remote-syslog-severity
    Remote Syslog Severity: warning

Server /cimc/log #
```

System Event Log

システム イベント ログの表示

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope sel**	System Event Log（SEL; システム イベント ログ）コマンド モードを開始します。
ステップ 2	Server /sel # **show entries [detail]**	システム イベントについて、タイムスタンプ、イベントの重大度、およびイベントの説明を表示します。

	コマンドまたはアクション	目的
		detail キーワードを指定すると、表形式ではなくリスト形式で情報が表示されます。

次に、システム イベント ログを表示する例を示します。

```
Server# scope sel
Server /sel # show entries
Time                 Severity      Description
-------------------- ------------- ----------------------------------------
[System Boot]      Informational " LED_PSU_STATUS: Platform sensor, OFF event was asserted"

[System Boot]       Informational " LED_HLTH_STATUS: Platform sensor, GREEN was asserted"
[System Boot]       Normal        " PSU_REDUNDANCY: PS Redundancy sensor, Fully Redundant
was asserted"
[System Boot]       Normal        " PSU2 PSU2_STATUS: Power Supply sensor for PSU2, Power
Supply input lost (AC/DC) was deasserted"
[System Boot]       Informational " LED_PSU_STATUS: Platform sensor, ON event was asserted"

[System Boot]       Informational " LED_HLTH_STATUS: Platform sensor, AMBER was asserted"
[System Boot]       Critical      " PSU_REDUNDANCY: PS Redundancy sensor, Redundancy Lost
was asserted"
[System Boot]       Critical      " PSU2 PSU2_STATUS: Power Supply sensor for PSU2, Power
Supply input lost (AC/DC) was asserted"
[System Boot]       Normal        " HDD_01_STATUS: Drive Slot sensor, Drive Presence was
asserted"
[System Boot]       Critical      " HDD_01_STATUS: Drive Slot sensor, Drive Presence was
deasserted"
[System Boot]       Informational " DDR3_P2_D1_INFO: Memory sensor, OFF event was asserted"

2001-01-01 08:30:16 Warning       " PSU2 PSU2_VOUT: Voltage sensor for PSU2, failure event
 was deasserted"
2001-01-01 08:30:16 Critical     " PSU2 PSU2_VOUT: Voltage sensor for PSU2, non-recoverable
 event was deasserted"
2001-01-01 08:30:15 Informational " LED_PSU_STATUS: Platform sensor, ON event was asserted"

2001-01-01 08:30:15 Informational " LED_HLTH_STATUS: Platform sensor, AMBER was asserted"
2001-01-01 08:30:15 Informational " LED_HLTH_STATUS: Platform sensor, FAST BLINK event was
 asserted"
2001-01-01 08:30:14 Non-Recoverable " PSU2 PSU2_VOUT: Voltage sensor for PSU2, non-recoverable
 event was asserted"
2001-01-01 08:30:14 Critical      " PSU2 PSU2_VOUT: Voltage sensor for PSU2, failure event
 was asserted"
--More--
```

システム イベント ログのクリア

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope sel**	システム イベント ログ コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	Server /sel # **clear**	処理の確認を求めるプロンプトが表示されます。プロンプトに **y** と入力すると、システム イベント ログはクリアされます。

次に、システム イベント ログをクリアする例を示します。

```
Server# scope sel
Server /sel # clear
This operation will clear the whole sel.
Continue?[y|N]y
```

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，162 ページ
- BIOS CMOS のクリア，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，166 ページ

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。

重要 ファームウェアまたは BIOS の更新が進行中の場合は、それらのタスクが完了するまで、テクニカル サポート データをエクスポートしないでください。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope tech-support**	テクニカル サポート コマンド モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	Server /cimc/tech-support # **set tftp-ip** *ip-address*	テクニカル 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 アドレスを指定します。
ステップ 4	Server /cimc/tech-support # **set path** *path/filename*	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を指定します。 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。 **ヒント** システムがファイル名を自動生成するようには default.tar.gz というファイル名を入力します。
ステップ 5	Server /cimc/tech-support # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 6	Server /cimc/tech-support # **start**	TFTP サーバへのデータ ファイルの転送を開始します。
ステップ 7	Server /cimc/tech-support # **cancel**	（任意） TFTP サーバへのデータ ファイルの転送をキャンセルします。

次に、テクニカル サポート データ ファイルを作成し、そのファイルを TFTP サーバに転送する例を示します。

```
Server# scope cimc
Server /cimc # scope tech-support
Server /cimc/tech-support # set tftp-ip 192.0.20.41
Server /cimc/tech-support *# set path /user/user1/default.tar.gz
Server /cimc/tech-support *# commit
Server /cimc/tech-support # start
Tech Support upload started.
```

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。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **reboot**	CIMC を再起動します。

次に、CIMC を再起動する例を示します。

```
Server# scope cimc
Server /cimc # reboot
```

BIOS CMOS のクリア

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、サーバの BIOS CMOS メモリのクリア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。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope bios**	bios コマンド モードを開始します。
ステップ 2	Server /bios # **clear-cmos**	確認を求めるプロンプトの後に、CMOS メモリがクリアされます。

次に、BIOS CMOS メモリをクリアする例を示します。

```
Server# scope bios
Server /bios # clear-cmos

This operation will clear the BIOS CMOS.
Note: Server should be in powered off state to clear CMOS.
Continue?[y|n] y

Server /bios #
```

破損した BIOS のリカバリ

（注） この手順は、一部のサーバ モデルでは使用できません。

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

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

はじめる前に

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

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope bios**	bios コマンド モードを開始します。
ステップ 2	Server# **recover**	BIOS リカバリ イメージのロードに関するダイアログを起動します。

次に、破損した BIOS を回復する例を示します。

```
Server# scope bios
Server /bios # recover
This operation will automatically power on the server to perform BIOS FW recovery.
Continue?[y|N]y
```

次の作業

電源を再投入するか、サーバをリセットします。

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。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **factory-default**	確認プロンプトの後に、CIMC が出荷時デフォルトにリセットされます。

CIMC の出荷時デフォルトには、次の条件が含まれます。

- CIMC CLI へのアクセス用に、SSH がイネーブルになっている。 Telnet はディセーブルになります。
- CIMC GUI へのアクセス用に、HTTPS がイネーブルになっている。
- 単一のユーザ アカウントが存在している（ユーザ名は **admin**、パスワードは **password**）。
- 管理ポートで DHCP がイネーブルになっている。
- ブート順が EFI、CDROM、PXE（LoM を使用）、FDD、HDD になっている。
- KVM と vMedia がイネーブルになっている。
- USB がイネーブルになっている。
- SoL がディセーブルになっている。

次に、CIMC を出荷時デフォルトにリセットする例を示します。

```
Server# scope cimc
Server /cimc # factory-default
This operation will reset the CIMC configuration to factory default.
All your configuration will be lost.
Continue?[y|N]
```

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作成し、生成された 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保存されるのは、管理プレーンからの情報だけです。サーバ上のデータはバックアップされません。ユーザ アカウントやサーバ証明書など、機密情報の設定はエクスポートされません。

エクスポートされた CIMC 設定ファイルは、同じシステムで復元したり、別の CIMC システムにインポートしたりできます。ただし、インポートするシステムのソフトウェア バージョンとエクスポートするシステムのソフトウェア バージョンが同じであるか、両者の設定に互換性があることが前提となります。 設定ファイルを設定テンプレートとして他のシステムにインポートする場合は、IP アドレスやホスト名などシステム固有の設定を変更する必要があります。 インポート操作によって情報が変更されるのは、管理プレーンだけです。

CIMC 設定ファイルは XML テキスト ファイルで、その構造と要素は CIMC コマンド モードに対応しています。

エクスポートまたはインポート操作を実行する場合は、次のガイドラインを考慮してください。

- エクスポートまたはインポートは、システムがアップ状態で、稼働しているときに実行できます。 エクスポート操作によるサーバまたはネットワーク トラフィックへの影響はありませんが、インポート操作によって IP アドレスなどが変更されると、トラフィックが中断されたりサーバがリブートされたりすることがあります。
- エクスポートとインポートを同時に実行することはできません。

CIMC 設定のエクスポート

（注） セキュリティ上の理由から、この操作でユーザ アカウントやサーバ証明書をエクスポートしないでください。

重要 ファームウェアまたは BIOS の更新が進行中の場合は、それらのタスクが完了するまで、CIMC 設定をエクスポートしないでください。

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

ネーブルであることを確認します。 コンフィギュレーションのエクスポート時に SNMP がディセーブルであると、ファイルをインポートしたときに CIMC によって SNMP 値が適用されません。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope import-export**	import-export コマンド モードを開始します。
ステップ 3	Server /cimc/import-export # **export-config** *tftp-ip-address path-and-filename*	バックアップ操作を開始します。 コンフィギュレーション ファイルは、指定した IP アドレスにある TFTP サーバ上に指定したパスとファイル名で保存されます。

エクスポート操作が正常に完了したかどうかを確認するには、**show detail** コマンドを使用します。操作を中止するには、CTRL+C を入力します。

次に、CIMC コンフィギュレーション ファイルをバックアップする例を示します。

```
Server# scope cimc
Server /cimc # scope import-export
Server /cimc/import-export # export-config 192.0.2.34 /ucs/backups/cimc5.xml
Export config started. Please check the status using "show detail".
Server /cimc/import-export # show detail
Import Export:
    Operation: EXPORT
    Status: COMPLETED
    Error Code: 100 (No Error)
    Diagnostic Message: NONE

Server /cimc/import-export #
```

CIMC 設定のインポート

重要 ファームウェアまたはBIOSの更新が進行中の場合は、それらのタスクが完了するまで、CIMC設定をインポートしないでください。

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 設定情報を復元したい場合は、インポートを実行する前に、このサーバで SNMP がディセーブルであることを確認します。インポートを実行するときにSNMPがイネーブルであると、CIMCは現在の値を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しません。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope cimc**	CIMC コマンド モードを開始します。
ステップ 2	Server /cimc # **scope import-export**	import-export コマンド モードを開始します。
ステップ 3	Server /cimc/import-export # **import-config** *tftp-ip-address path-and-filename*	インポート操作を開始します。 指定した IP アドレスにある TFTP サーバ上の、指定したパスとファイル名のコンフィギュレーション ファイルがインポートされます。

インポート操作が正常に完了したかどうかを確認するには、**show detail** コマンドを使用します。操作を中止するには、CTRL+C を入力します。

次に、CIMC コンフィギュレーションをインポートする方法を示します。

```
Server# scope cimc
Server /cimc # scope import-export
Server /cimc/import-export # import-config 192.0.2.34 /ucs/backups/cimc5.xml
Import config started. Please check the status using "show detail".
Server /cimc/import-export #
```

付 録 A

サーバ モデル別 BIOS パラメータ

この付録の内容は、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，202 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] **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] **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] **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] **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は自動的には上がりません。 • [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] **set EnhancedIntelSpeedStep**	プロセッサで Enhanced Intel SpeedStep Technology を使用するかどうか。このテクノロジーでは、プロセッサの電圧やコア周波数をシステムが動的に調整できます。 このテクノロジーにより、平均電力消費量と平均熱発生量が減少する可能性があります。 次のいずれかになります。 • [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] **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] **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] **set ExecuteDisable**	アプリケーション コードを実行できる場所を指定するために、サーバのメモリ領域を分類します。 この分類の結果、悪意のあるワームがバッファにコードを挿入しようとした場合、プロセッサでコードの実行をディセーブルにします。 この設定は、損害、ワームの増殖、および特定クラスの悪意のあるバッファ オーバーフロー攻撃を防止するのに役立ちます。 次のいずれかになります。 • [Disabled]：プロセッサでメモリ領域を分類しません。 • [Enabled]：プロセッサでメモリ領域を分類します。 オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。

名前	説明
[Intel Virtualization Technology] **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]：プロセッサで、複数のオペレーティング システムをそれぞれ独立したパーティション内で実行できます。 （注） このオプションを変更した場合は、設定を有効にするためにサーバの電源を再投入する必要があります。
[Intel VT for Directed IO] **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]：プロセッサで仮想化テクノロジーを使用しません。 • [Enabled]：プロセッサで仮想化テクノロジーを使用します。
[Intel VT-d Interrupt Remapping] **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] **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] **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] **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] **set DirectCacheAccess**	プロセッサで、データを I/O デバイスから直接プロセッサ キャッシュに入れることにより、I/O パフォーマンスを向上させることができます。 この設定はキャッシュ ミスを減らすのに役立ちます。 次のいずれかになります。 • [Disabled]：データは I/O デバイスから直接プロセッサ キャッシュには入れられません。 • [Enabled]：データは I/O デバイスから直接プロセッサ キャッシュに入れられます。
[Processor C3 Report] **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：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：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] **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] **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 だけ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：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がイネーブルになります。 この設定はハイ パフォーマンス コンピューティングとも呼ばれます。 • [Custom]：パフォーマンス プロファイルのすべてのオプションをサーバの BIOS セットアップから設定できます。 また、Hardware Prefetcher オプションと Adjacent Cache-Line Prefetch オプションは、下記のフィールドで設定できます。

名前	説明
[Hardware Prefetcher] **set HardwarePrefetch**	プロセッサで、インテル ハードウェア プリフェッチャが必要に応じてデータおよび命令ストリームをメモリから取得し、統合 2 次キャッシュに入れることを許可するかどうか。 次のいずれかになります。 • [Disabled]：ハードウェア プリフェッチャは使用しません。 • [Enabled]：プロセッサで、キャッシュの問題が検出されたときにプリフェッチャを使用します。 （注） この値を指定するには、CPUPerformance を [Custom] に設定する必要があります。 [Custom] 以外の値の場合は、このオプションよりも、選択された CPU パフォーマンス プロファイルの設定が優先されます。
[Adjacent Cache-Line Prefetch] **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、CPUPerformance を [Custom] に設定する必要があります。 [Custom] 以外の値の場合は、このオプションよりも、選択された CPU パフォーマンス プロファイルの設定が優先されます。
[CPU C State] **set ProcessorCcxEnable**	アイドル期間中にシステムが省電力モードに入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時でもハイ パフォーマンス状態のままになります。 • [Enabled]：システムは DIMM や CPU などのシステム コンポーネントへの電力を低減できます。 電力低減量は、**set PackageCStateLimit** コマンドで指定します。

名前	説明
[C1E] **set ProcessorC1eEnable**	C1 ステートに入ったときに、CPU が最小周波数に移行するかどうか。 次のいずれかになります。 • [Disabled]：CPU は C1 ステートでも引き続き最大周波数で動作します。 • [Enabled]：CPU は最小周波数に移行します。 このオプションでは C1 ステートで節約される電力量が最大になります。 （注） このオプションは、ProcessorCcxEnable がイネーブルの場合にのみ使用します。
[OEM AESNI] **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] **set SelectMemoryRAS**	サーバに対するメモリの Reliability, Availability, and Serviceability（RAS）の設定方法。 次のいずれかになります。 • 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]：システムは、DIMM に障害が発生した場合に使用するためのメモリを予約します。 障害が発生した場合、サーバは DIMM をオフラインにして、予約済みのメモリと置き換えます。 このオプションは、ミラーリングよりも冗長性が低くなりますが、サーバで実行するプログラムに使用できるメモリの量が多くなります。

名前	説明
[NUMA Optimized] **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] **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：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：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] **set OnboardSATA**	プロセッサで組み込み 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 コントローラを使用しません。 • [Enabled]：プロセッサで組み込み SATA コントローラを使用します。

名前	説明
[SATA Mode] **set ConfigSATAMode**	SATA コントローラが動作するモード。 次のいずれかになります。 • [AHCI]：コントローラでは 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]：コントローラでは AHCI と RAID の両方がディセーブルになり、IDE エミュレーション モードで動作します。 • [Enhanced]：コントローラはで AHCI と RAID の両方がイネーブルになります。 • [S/W RAID]：コントローラでは 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] **set Serial-PortA**	シリアル ポート A がイネーブルかディセーブルか。 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] **set SerialPortAAddress**	シリアル ポート A がイネーブルの場合は、使用する 16 進数の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] **set Serial-PortB**	シリアル ポート B がイネーブルかディセーブルか。 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] **set SerialPortBAddress**	シリアル ポート B がイネーブルの場合は、使用する 16 進数の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] **set USBController**	プロセッサで組み込み 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]：サーバで組み込み USB コントローラを使用しません。 • [Enabled]：プロセッサで組み込み USB コントローラを使用します。
[Make Device Non-Bootable] **set MakeUSBDeviceNonBootable**	サーバが 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]：サーバは USB デバイスからブートできます。 • [Enabled]：サーバは USB デバイスからブートできません。
[USB Performance Mode] **set USBPerformanceMode**	サーバで USB 2.0 または 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り、USB デバイスはすべて USB 2.0 モードで機能します。 このオプションでは、USB デバイスのパフォーマンスが最大化されますが、追加の電力が必要となります。 • [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り、USB デバイスはすべて USB 1.1 モードで機能します。 このオプションでは、必要な電力が少なくなりますが、USB デバイスのパフォーマンスは低下します。

[PCI Configuration] のパラメータ

名前	説明
[Memory Mapped I/O Above 4GB] **set MemoryMappedIOAbove4GB**	64 ビット PCI デバイスの 4 GB 以上のアドレス空間に対するメモリ マップド I/O をイネーブルにするか、ディセーブルにするか。 レガシーなオプション ROM は 4 GB を超えるアドレスにアクセスできません。 PCI デバイスが 64 ビット対応でも、レガシーなオプション ROM を使用する場合は、この設定をイネーブルにしても正しく機能しない場合があります。 次のいずれかになります。 • [Disabled]：サーバでは 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングしません。 • [Enabled]：サーバで 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングします。
[Onboard Gb NIC 1] **set OnboardNic1**	サーバ上の 1 番目のオンボード ネットワーク インターフェイス カード（NIC）がイネーブルかディセーブルか。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] **set OnboardNic2**	サーバ上の 2 番目のオンボード NIC がイネーブルかディセーブルか。 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] **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] **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 を使用できません。 • [Enabled]：PCIe オプション ROM を使用できます。
[PCIe Slot *n* ROM] **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* を使用できません。 • [Enabled]：拡張スロット *n* を使用できます。
[PCIe Mezzanine Slot ROM] **set SlotMezzDisable**	PCIe メザニン スロットの拡張 ROM をサーバで使用できるかどうか。 次のいずれかになります。 • [Disabled]：メザニン スロットを使用できません。 • [Enabled]：メザニン スロットを使用できます。
[Active Video] **set ActiveVideo**	サーバでのビデオの表示方法。 次のいずれかになります。 • [Auto]：使用可能な場合、サーバで外部グラフィックス アダプタを表示用に使用します。 • Onboard_Device：外部グラフィックス アダプタが使用可能な場合でも、サーバでは常に内部グラフィックス アダプタを使用します。

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] **set AssertNMIOnSERR**	システムエラー（SERR）の発生時に、BIOSがマスク不能割り込み（NMI）を生成し、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 は NMI を生成することもエラーをログに記録することもしません。 • [Enabled]：SERR の発生時に、BIOS は NMI を生成し、エラーをログに記録します。 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] **set AssertNMIOnPERR**	プロセッサ バス パリティ エラー（PERR）の発生時に、BIOSがマスク不能割り込み（NMI）を生成し、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 は NMI を生成することもエラーをログに記録することもしません。 • [Enabled]：PERR の発生時に、BIOS は 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 をイネーブルにする必要があります。
[FRB2 Enable] **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 によって FRB2 タイマーが使用されるかどうか。 次のいずれかになります。 • [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の回復に使用されます。

名前	説明
[PlugNPlay BMC Detection] **set BMCPnP**	システムが 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]：システムは BMC を自動的に検出しません。 • [Enabled]：システムは可能な場合は常に BMC を自動的に検出します。
[ACPI1.0 Support] **set ACPI10Support**	BIOS が FADT の ACPI 1.0 バージョンを Root System Description Table にパブリッシュするかどうか。 このバージョンは、ACPI 1.0 だけをサポートする OS バージョンとの互換性を保つために必要となる場合があります。 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 バージョンがパブリッシュされます。
[Console Redirection] **set ConsoleRedir**	POST および BIOS のブート中に、シリアル ポートをコンソール リダイレクションに使用できるようにします。 BIOS のブートが完了し、オペレーティング システムがサーバを担当すると、コンソール リダイレクションは関連がなくなり、無効になります。 次のいずれかになります。 • [Disabled]：POST 中にコンソール リダイレクションは発生しません。 • Serial_Port_A：POST 中のコンソール リダイレクション用にシリアル ポート A を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場合は、POST 中に表示される Quiet Boot のロゴ画面もディセーブルにします。

名前	説明
[Flow Control] **set FlowCtrl**	フロー制御にハンドシェイク プロトコルを使用するかどうか。 送信要求/クリア ツー センド（RTS/CTS）を使用すると、隠れた端末問題が原因で発生する可能性があるフレーム コリジョンを減らすことができます。 次のいずれかになります。 • [None]：フロー制御は使用されません。 • [RTS-CTS]：RTS/CTS がフロー制御に使用されます。 （注） この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。
[Baud Rate] **set BaudRate**	シリアル ポートの伝送速度として使用されるボー レート。 [Console Redirection] をディセーブルにした場合は、このオプションを使用できません。 次のいずれかになります。 • [9.6k]：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 アプリケーション上の設定と一致している必要があります。

名前	説明
[Terminal Type] **set TerminalType**	コンソール リダイレクションに使用される文字フォーマットのタイプ。 次のいずれかになります。 • [PC-ANSI]：PC-ANSI端末フォントが使用されます。 • [VT100]：サポートされている vt100 ビデオ端末とその文字セットが使用されます。 • [VT100-PLUS]：サポートされている vt100-plus ビデオ端末とその文字セットが使用されます。 • [VT-UTF8]：UTF-8 文字セットのビデオ端末が使用されます。 （注） この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。
[Legacy OS Redirection] **set LegacyOSRedir**	シリアル ポートでレガシーなオペレーティング システム（DOSなど）からのリダイレクションを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 リダイレクションがイネーブルになっているシリアルポートは、レガシーなオペレーティング システムから認識されません。 • [Enabled]：コンソール リダイレクションがイネーブルになっているシリアルポートは、レガシーなオペレーティング システムから認識できます。

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] **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] **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] **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] **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は自動的には上がりません。 • [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] **set EnhancedIntelSpeedStep**	プロセッサで Enhanced Intel SpeedStep Technology を使用するかどうか。このテクノロジーでは、プロセッサの電圧やコア周波数をシステムが動的に調整できます。 このテクノロジーにより、平均電力消費量と平均熱発生量が減少する可能性があります。 次のいずれかになります。 • [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] **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] **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] **set ExecuteDisable**	アプリケーション コードを実行できる場所を指定するために、サーバのメモリ領域を分類します。 この分類の結果、悪意のあるワームがバッファにコードを挿入しようとした場合、プロセッサでコードの実行をディセーブルにします。 この設定は、損害、ワームの増殖、および特定クラスの悪意のあるバッファ オーバーフロー攻撃を防止するのに役立ちます。 次のいずれかになります。 • [Disabled]：プロセッサでメモリ領域を分類しません。 • [Enabled]：プロセッサでメモリ領域を分類します。 オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。

名前	説明
[Intel Virtualization Technology] **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]：プロセッサで、複数のオペレーティング システムをそれぞれ独立したパーティション内で実行できます。 （注） このオプションを変更した場合は、設定を有効にするためにサーバの電源を再投入する必要があります。
[Intel VT for Directed IO] **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]：プロセッサで仮想化テクノロジーを使用しません。 • [Enabled]：プロセッサで仮想化テクノロジーを使用します。
[Intel VT-d Interrupt Remapping] **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] **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] **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] **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] **set DirectCacheAccess**	プロセッサで、データを I/O デバイスから直接プロセッサ キャッシュに入れることにより、I/O パフォーマンスを向上させることができます。 この設定はキャッシュ ミスを減らすのに役立ちます。 次のいずれかになります。 • [Disabled]：データは I/O デバイスから直接プロセッサ キャッシュには入れられません。 • [Enabled]：データは I/O デバイスから直接プロセッサ キャッシュに入れられます。
[Processor C3 Report] **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：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：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] **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] **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 だけ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：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がイネーブルになります。 この設定はハイ パフォーマンス コンピューティングとも呼ばれます。 • [Custom]：パフォーマンス プロファイルのすべてのオプションをサーバの BIOS セットアップから設定できます。 また、Hardware Prefetcher オプションと Adjacent Cache-Line Prefetch オプションは、下記のフィールドで設定できます。

名前	説明
[Hardware Prefetcher] **set HardwarePrefetch**	プロセッサで、インテル ハードウェア プリフェッチャが必要に応じてデータおよび命令ストリームをメモリから取得し、統合 2 次キャッシュに入れることを許可するかどうか。 次のいずれかになります。 • [Disabled]：ハードウェア プリフェッチャは使用しません。 • [Enabled]：プロセッサで、キャッシュの問題が検出されたときにプリフェッチャを使用します。 （注） この値を指定するには、CPUPerformance を [Custom] に設定する必要があります。 [Custom] 以外の値の場合は、このオプションよりも、選択された CPU パフォーマンス プロファイルの設定が優先されます。
[Adjacent Cache-Line Prefetch] **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、CPUPerformance を [Custom] に設定する必要があります。 [Custom] 以外の値の場合は、このオプションよりも、選択された CPU パフォーマンス プロファイルの設定が優先されます。
[CPU C State] **set ProcessorCcxEnable**	アイドル期間中にシステムが省電力モードに入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時でもハイ パフォーマンス状態のままになります。 • [Enabled]：システムは DIMM や CPU などのシステム コンポーネントへの電力を低減できます。 電力低減量は、**set PackageCStateLimit** コマンドで指定します。

名前	説明
[C1E] **set ProcessorC1eEnable**	C1 ステートに入ったときに、CPU が最小周波数に移行するかどうか。 次のいずれかになります。 • [Disabled]：CPU は C1 ステートでも引き続き最大周波数で動作します。 • [Enabled]：CPU は最小周波数に移行します。 このオプションでは C1 ステートで節約される電力量が最大になります。 （注） このオプションは、ProcessorCcxEnable がイネーブルの場合にのみ使用します。
[Spread Spectrum] **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] **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] **set SelectMemoryRAS**	サーバに対するメモリの Reliability, Availability, and Serviceability（RAS）の設定方法。 次のいずれかになります。 • 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]：システムは、DIMM に障害が発生した場合に使用するためのメモリを予約します。 障害が発生した場合、サーバはDIMM をオフラインにして、予約済みのメモリと置き換えます。 このオプションは、ミラーリングよりも冗長性が低くなりますが、サーバで実行するプログラムに使用できるメモリの量が多くなります。
[NUMA Optimized] **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] **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：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：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] **set Serial-PortA**	シリアル ポート A がイネーブルかディセーブルか。 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] **set SerialPortAAddress**	シリアル ポート A がイネーブルの場合は、使用する 16 進数の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] **set USBController**	プロセッサで組み込み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]：サーバで組み込み USB コントローラを使用しません。 • [Enabled]：プロセッサで組み込み USB コントローラを使用します。
[Make Device Non-Bootable] **set MakeUSBDeviceNonBootable**	サーバが 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]：サーバは USB デバイスからブートできます。 • [Enabled]：サーバは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] **set MemoryMappedIOAbove4GB**	64 ビット PCI デバイスの 4 GB 以上のアドレス空間に対するメモリ マップド I/O をイネーブルにするか、ディセーブルにするか。 レガシーなオプション ROM は 4 GB を超えるアドレスにアクセスできません。 PCI デバイスが 64 ビット対応でも、レガシーなオプション ROM を使用する場合は、この設定をイネーブルにしても正しく機能しない場合があります。 次のいずれかになります。 • [Disabled]：サーバでは 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングしません。 • [Enabled]：サーバで 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングします。
[Onboard Gb NIC 1] **set OnboardNic1**	サーバ上の 1 番目のオンボード ネットワーク インターフェイス カード（NIC）がイネーブルかディセーブルか。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] **set OnboardNic2**	サーバ上の 2 番目のオンボード NIC がイネーブルかディセーブルか。 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] **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] **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 を使用できません。 • [Enabled]：PCIe オプション ROM を使用できます。
[PCIe Slot *n* ROM] **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* を使用できません。 • [Enabled]：拡張スロット *n* を使用できます。
[Active Video] **set ActiveVideo**	サーバでのビデオの表示方法。 次のいずれかになります。 • [Auto]：使用可能な場合、サーバで外部グラフィックス アダプタを表示用に使用します。 • Onboard_Device：外部グラフィックス アダプタが使用可能な場合でも、サーバでは常に内部グラフィックス アダプタを使用します。

C250 サーバのサーバ管理 BIOS パラメータ

名前	説明
[Assert NMI on SERR] **set AssertNMIOnSERR**	システム エラー（SERR）の発生時に、BIOS がマスク不能割り込み（NMI）を生成し、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 は NMI を生成することもエラーをログに記録することもしません。 • [Enabled]：SERR の発生時に、BIOS は NMI を生成し、エラーをログに記録します。 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] **set AssertNMIOnPERR**	プロセッサ バス パリティ エラー（PERR）の発生時に、BIOS がマスク不能割り込み（NMI）を生成し、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 は NMI を生成することもエラーをログに記録することもしません。 • [Enabled]：PERR の発生時に、BIOS は 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 をイネーブルにする必要があります。
[FRB2 Enable] **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 によって FRB2 タイマーが使用されるかどうか。 次のいずれかになります。 • [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の回復に使用されます。
[PlugNPlay BMC Detection] **set BMCPnP**	システムが 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]：システムは BMC を自動的に検出しません。 • [Enabled]：システムは可能な場合は常に BMC を自動的に検出します。
[ACPI1.0 Support] **set ACPI10Support**	BIOS が FADT の ACPI 1.0 バージョンを Root System Description Table にパブリッシュするかどうか。 このバージョンは、ACPI 1.0 だけをサポートする OS バージョンとの互換性を保つために必要となる場合があります。 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 バージョンがパブリッシュされます。

名前	説明
[Console Redirection] **set ConsoleRedir**	POST および BIOS のブート中に、シリアル ポートをコンソール リダイレクションに使用できるようにします。BIOS のブートが完了し、オペレーティング システムがサーバを担当すると、コンソール リダイレクションは関連がなくなり、無効になります。次のいずれかになります。 • [Disabled]：POST 中にコンソール リダイレクションは発生しません。 • Serial_Port_A：POST 中のコンソール リダイレクション用にシリアル ポート A を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場合は、POST 中に表示される Quiet Boot のロゴ画面もディセーブルにします。
[Flow Control] **set FlowCtrl**	フロー制御にハンドシェイク プロトコルを使用するかどうか。送信要求/クリア ツー センド（RTS/CTS）を使用すると、隠れた端末問題が原因で発生する可能性があるフレーム コリジョンを減らすことができます。次のいずれかになります。 • [None]：フロー制御は使用されません。 • [RTS-CTS]：RTS/CTS がフロー制御に使用されます。 （注） この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。

名前	説明
[Baud Rate] **set BaudRate**	シリアル ポートの伝送速度として使用されるボー レート。 [Console Redirection] をディセーブルにした場合は、このオプションを使用できません。 次のいずれかになります。 • [9.6k]：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 アプリケーション上の設定と一致している必要があります。
[Terminal Type] **set TerminalType**	コンソール リダイレクションに使用される文字フォーマットのタイプ。 次のいずれかになります。 • [PC-ANSI]：PC-ANSI端末フォントが使用されます。 • [VT100]：サポートされている vt100 ビデオ端末とその文字セットが使用されます。 • [VT100-PLUS]：サポートされている vt100-plus ビデオ端末とその文字セットが使用されます。 • [VT-UTF8]：UTF-8 文字セットのビデオ端末が使用されます。 （注） この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。
[Legacy OS Redirection] **set LegacyOSRedir**	シリアル ポートでレガシーなオペレーティング システム（DOSなど）からのリダイレクションを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 リダイレクションがイネーブルになっているシリアルポートは、レガシーなオペレーティング システムから認識されません。 • [Enabled]：コンソール リダイレクションがイネーブルになっているシリアルポートは、レガシーなオペレーティング システムから認識できます。

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] **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] **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] **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は自動的には上がりません。 • [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] **set EnhancedIntelSpeedStep**	プロセッサで Enhanced Intel SpeedStep Technology を使用するかどうか。このテクノロジーでは、プロセッサの電圧やコア周波数をシステムが動的に調整できます。 このテクノロジーにより、平均電力消費量と平均熱発生量が減少する可能性があります。 次のいずれかになります。 • [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] **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] **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] **set ExecuteDisable**	アプリケーション コードを実行できる場所を指定するために、サーバのメモリ領域を分類します。 この分類の結果、悪意のあるワームがバッファにコードを挿入しようとした場合、プロセッサでコードの実行をディセーブルにします。 この設定は、損害、ワームの増殖、および特定クラスの悪意のあるバッファ オーバーフロー攻撃を防止するのに役立ちます。 次のいずれかになります。 • [Disabled]：プロセッサでメモリ領域を分類しません。 • [Enabled]：プロセッサでメモリ領域を分類します。 オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。

名前	説明
[Intel Virtualization Technology] **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]：プロセッサで、複数のオペレーティング システムをそれぞれ独立したパーティション内で実行できます。 （注） このオプションを変更した場合は、設定を有効にするためにサーバの電源を再投入する必要があります。
[Intel VT for Directed IO] **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]：プロセッサで仮想化テクノロジーを使用しません。 • [Enabled]：プロセッサで仮想化テクノロジーを使用します。
[Intel VT-d Interrupt Remapping] **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] **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] **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] **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] **set DirectCacheAccess**	プロセッサで、データを I/O デバイスから直接プロセッサ キャッシュに入れることにより、I/O パフォーマンスを向上させることができます。 この設定はキャッシュ ミスを減らすのに役立ちます。 次のいずれかになります。 • [Disabled]：データは I/O デバイスから直接プロセッサ キャッシュには入れられません。 • [Enabled]：データは I/O デバイスから直接プロセッサ キャッシュに入れられます。
[Processor C3 Report] **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：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：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] **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] **set PackageCStateLimit**	アイドル時にサーバ コンポーネントが使用できる電力量。 次のいずれかになります。 • C0_state：サーバはすべてのサーバ コンポーネントに常にフル パワーを提供します。 このオプションでは、最高レベルのパフォーマンスが維持され、最大量の電力が必要となります。 • C1_state：CPU のアイドル時に、システムは電力消費を少し減らします。 このオプションでは、必要な電力が C0 よりも少なく、サーバはすばやくハイ パフォーマンス モードに戻ることができます。 • C3_state：CPU のアイドル時に、システムは C1 オプションの場合よりもさらに電力消費を減らします。 この場合、必要な電力は C1 または C0 よりも少なくなりますが、サーバがハイ パフォーマンス モードに戻るのに要する時間が少し長くなります。 • C6_state：CPU のアイドル時に、システムは C3 オプションの場合よりもさらに電力消費を減らします。 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：CPU のアイドル時に、サーバはコンポーネントが使用できる電力量を最小にします。 このオプションでは、節約される電力量が最大になりますが、サーバがハイ パフォーマンス モードに戻るのに要する時間も最も長くなります。 • No_Limit：サーバは、使用可能な任意の C ステートに入ることがあります。 （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されます。
[CPU C State] **set ProcessorCcxEnable**	アイドル期間中にシステムが省電力モードに入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時でもハイ パフォーマンス状態のままになります。 • [Enabled]：システムは DIMM や CPU などのシステム コンポーネントへの電力を低減できます。 電力低減量は、**set PackageCStateLimit** コマンドで指定します。

名前	説明
[C1E] **set ProcessorC1eEnable**	C1 ステートに入ったときに、CPU が最小周波数に移行するかどうか。 次のいずれかになります。 • [Disabled]：CPU は C1 ステートでも引き続き最大周波数で動作します。 • [Enabled]：CPU は最小周波数に移行します。 このオプションでは C1 ステートで節約される電力量が最大になります。 （注） このオプションは、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] **set SelectMemoryRAS**	サーバに対するメモリの Reliability, Availability, and Serviceability（RAS）の設定方法。 次のいずれかになります。 • 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]：システムは、DIMM に障害が発生した場合に使用するためのメモリを予約します。 障害が発生した場合、サーバは DIMM をオフラインにして、予約済みのメモリと置き換えます。 このオプションは、ミラーリングよりも冗長性が低くなりますが、サーバで実行するプログラムに使用できるメモリの量が多くなります。

名前	説明
[NUMA Optimized] **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] **set SparingMode**	CIMC で使用される予備設定モード。 次のいずれかになります。 • Rank_Sparing：ランク レベルで予備メモリが割り当てられます。 • [DIMM Sparing]：DIMM レベルで予備メモリが割り当てられます。 （注） このオプションは、set SelectMemoryRAS が [Sparing] に設定されている場合にのみ使用されます。
[Mirroring Mode] **set MirroringMode**	ミラーリングは Integrated Memory Controller（IMC）全体でサポートされ、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ます。 次のいずれかになります。 • [Intersocket]：各 IMC は 2 つのソケット全体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、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] **set PatrolScrub**	システムがサーバ上のメモリの未使用部分でも単一ビット メモリ エラーをアクティブに探して訂正するかどうか。 次のいずれかになります。 • [Disabled]：CPU がメモリ アドレスの読み取りまたは書き込みを行うときのみ、システムはメモリの ECC エラーをチェックします。 • [Enabled]：システムは定期的にメモリを読み書きして ECC エラーを探します。 エラーが見つかると、システムは修正を試みます。 このオプションにより、単一ビット エラーは複数ビット エラーになる前に修正される場合がありますが、パトロール スクラブの実行時にパフォーマンスが低下する場合もあります。
[Patrol Scrub Interval] **set PatrolScrubDuration**	各パトロール スクラブによるメモリ アクセスの時間間隔を制御します。 小さくすると、メモリのスクラブ頻度が高くなりますが、必要なメモリ帯域幅も多くなります。 5 ～ 23 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] **set CKELowPolicy**	DIMM の省電力モード ポリシーを制御します。 次のいずれかになります。 • [Disabled]：DIMM は省電力モードに入りません。 • [Slow]：DIMM は省電力モードに入ることができますが、要件が厳しくなります。 したがって、DIMM が省電力モードに入る頻度は低くなります。 • [Fast]：DIMM はできる限り頻繁に省電力モードに入ります。 • [Auto]：BIOS は DIMM の構成に基づいて DIMM が省電力モードに入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] **set Serial-PortA**	シリアル ポート A がイネーブルかディセーブルか。 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] **set MakeUSBDeviceNonBootable**	サーバが 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]：サーバは USB デバイスからブートできます。 • [Enabled]：サーバは 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] **set MemoryMappedIOAbove4GB**	64 ビット PCI デバイスの 4 GB 以上のアドレス空間に対するメモリ マップド I/O をイネーブルにするか、ディセーブルにするか。 レガシーなオプション ROM は 4 GB を超えるアドレスにアクセスできません。 PCI デバイスが 64 ビット対応でも、レガシーなオプション ROM を使用する場合は、この設定をイネーブルにしても正しく機能しない場合があります。 次のいずれかになります。 • [Disabled]：サーバでは 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングしません。 • [Enabled]：サーバで 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングします。

名前	説明
[Onboard NIC *n* ROM] **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] **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 を使用できません。 • [Enabled]：PCIe オプション ROM を使用できます。
[PCIe Slot *n* ROM] **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* を使用できません。 • [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] **set AssertNMIOnSERR**	システムエラー（SERR）の発生時に、BIOS がマスク不能割り込み（NMI）を生成し、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 は NMI を生成することもエラーをログに記録することもしません。 • [Enabled]：SERR の発生時に、BIOS は NMI を生成し、エラーをログに記録します。 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] **set AssertNMIOnPERR**	プロセッサ バス パリティ エラー（PERR）の発生時に、BIOS がマスク不能割り込み（NMI）を生成し、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 は NMI を生成することもエラーをログに記録することもしません。 • [Enabled]：PERR の発生時に、BIOS は 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 をイネーブルにする必要があります。
[Console Redirection] **set ConsoleRedir**	POST および BIOS のブート中に、シリアル ポートをコンソール リダイレクションに使用できるようにします。 BIOS のブートが完了し、オペレーティング システムがサーバを担当すると、コンソール リダイレクションは関連がなくなり、無効になります。 次のいずれかになります。 • [Disabled]：POST 中にコンソール リダイレクションは発生しません。 • Serial_Port_A：POST 中のコンソール リダイレクション用にシリアル ポート A を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場合は、POST 中に表示される Quiet Boot のロゴ画面もディセーブルにします。
[Flow Control] **set FlowCtrl**	フロー制御にハンドシェイク プロトコルを使用するかどうか。 送信要求/クリア ツー センド（RTS/CTS）を使用すると、隠れた端末問題が原因で発生する可能性があるフレーム コリジョンを減らすことができます。 次のいずれかになります。 • [None]：フロー制御は使用されません。 • [RTS-CTS]：RTS/CTS がフロー制御に使用されます。 （注） この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。

名前	説明
[Baud Rate] **set BaudRate**	シリアル ポートの伝送速度として使用されるボー レート。 [Console Redirection] をディセーブルにした場合は、このオプションを使用できません。 次のいずれかになります。 • [9.6k]：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 アプリケーション上の設定と一致している必要があります。
[Terminal Type] **set TerminalType**	コンソール リダイレクションに使用される文字フォーマットのタイプ。 次のいずれかになります。 • [PC-ANSI]：PC-ANSI端末フォントが使用されます。 • [VT100]：サポートされている vt100 ビデオ端末とその文字セットが使用されます。 • [VT100-PLUS]：サポートされている vt100-plus ビデオ端末とその文字セットが使用されます。 • [VT-UTF8]：UTF-8 文字セットのビデオ端末が使用されます。 （注） この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。

名前	説明
[OS Boot Watchdog Timer Timeout] **set OSBootWatchdogTimerTimeOut**	BIOS でウォッチドッグ タイマーの設定に使用されるタイムアウト値。 次のいずれかになります。 • 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：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：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：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] **set OSBootWatchdogTimerPolicy**	ウォッチドッグ タイマーが切れた場合にシステムで実行されるアクション。 次のいずれかになります。 • 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] **set LegacyOSRedir**	シリアル ポートでレガシーなオペレーティング システム（DOS など）からのリダイレクションを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 リダイレクションがイネーブルになっているシリアル ポートは、レガシーなオペレーティング システムから認識されません。 • [Enabled]：コンソール リダイレクションがイネーブルになっているシリアル ポートは、レガシーなオペレーティング システムから認識できます。

名前	説明
[OS Boot Watchdog Timer] **set OSBootWatchdogTimer**	BIOS が指定されたタイムアウト値でウォッチドッグ タイマーをプログラムするかどうか。 次のいずれかになります。 • [Disabled]：サーバのブートにかかる時間をトラッキングするためにウォッチドッグタイマーは使用されません。 • [Enabled]：サーバのブートにかかる時間をウォッチドッグ タイマーでトラッキングします。 サーバが **set OSBootWatchdogTimerTimeout** コマンドで指定された時間内にブートしない場合、CIMC はエラーをログに記録し、**set OSBootWatchdogTimerPolicy** コマンドで指定されたアクションを実行します。

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] **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] **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] **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は自動的には上がりません。 • [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] **set EnhancedIntelSpeedStep**	プロセッサで Enhanced Intel SpeedStep Technology を使用するかどうか。このテクノロジーでは、プロセッサの電圧やコア周波数をシステムが動的に調整できます。 このテクノロジーにより、平均電力消費量と平均熱発生量が減少する可能性があります。 次のいずれかになります。 • [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] **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] **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] **set ExecuteDisable**	アプリケーション コードを実行できる場所を指定するために、サーバのメモリ領域を分類します。 この分類の結果、悪意のあるワームがバッファにコードを挿入しようとした場合、プロセッサでコードの実行をディセーブルにします。 この設定は、損害、ワームの増殖、および特定クラスの悪意のあるバッファ オーバーフロー攻撃を防止するのに役立ちます。 次のいずれかになります。 • [Disabled]：プロセッサでメモリ領域を分類しません。 • [Enabled]：プロセッサでメモリ領域を分類します。 オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。
[Intel Virtualization Technology] **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]：プロセッサで、複数のオペレーティング システムをそれぞれ独立したパーティション内で実行できます。 （注） このオプションを変更した場合は、設定を有効にするためにサーバの電源を再投入する必要があります。
[Intel VT for Directed IO] **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]：プロセッサで仮想化テクノロジーを使用しません。 • [Enabled]：プロセッサで仮想化テクノロジーを使用します。

名前	説明
[Intel VT-d Interrupt Remapping] **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] **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] **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] **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] **set DirectCacheAccess**	プロセッサで、データを I/O デバイスから直接プロセッサ キャッシュに入れることにより、I/O パフォーマンスを向上させることができます。 この設定はキャッシュ ミスを減らすのに役立ちます。 次のいずれかになります。 • [Disabled]：データは I/O デバイスから直接プロセッサ キャッシュには入れられません。 • [Enabled]：データは I/O デバイスから直接プロセッサ キャッシュに入れられます。
[Processor C3 Report] **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：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：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] **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] **set PackageCStateLimit**	アイドル時にサーバ コンポーネントが使用できる電力量。 次のいずれかになります。 • C0_state：サーバはすべてのサーバ コンポーネントに常にフル パワーを提供します。 このオプションでは、最高レベルのパフォーマンスが維持され、最大量の電力が必要となります。 • C1_state：CPU のアイドル時に、システムは電力消費を少し減らします。 このオプションでは、必要な電力が C0 よりも少なく、サーバはすばやくハイ パフォーマンス モードに戻ることができます。 • C3_state：CPU のアイドル時に、システムは C1 オプションの場合よりもさらに電力消費を減らします。 この場合、必要な電力は C1 または C0 よりも少なくなりますが、サーバがハイ パフォーマンス モードに戻るのに要する時間が少し長くなります。 • C6_state：CPU のアイドル時に、システムは C3 オプションの場合よりもさらに電力消費を減らします。 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：CPU のアイドル時に、サーバはコンポーネントが使用できる電力量を最小にします。 このオプションでは、節約される電力量が最大になりますが、サーバがハイ パフォーマンス モードに戻るのに要する時間も最も長くなります。 • No_Limit：サーバは、使用可能な任意の C ステートに入ることがあります。 （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されます。
[CPU C State] **set ProcessorCcxEnable**	アイドル期間中にシステムが省電力モードに入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時でもハイ パフォーマンス状態のままになります。 • [Enabled]：システムは DIMM や CPU などのシステム コンポーネントへの電力を低減できます。 電力低減量は、**set PackageCStateLimit** コマンドで指定します。

名前	説明
[C1E] **set ProcessorC1eEnable**	C1 ステートに入ったときに、CPU が最小周波数に移行するかどうか。 次のいずれかになります。 • [Disabled]：CPU は C1 ステートでも引き続き最大周波数で動作します。 • [Enabled]：CPU は最小周波数に移行します。 このオプションでは C1 ステートで節約される電力量が最大になります。 （注） このオプションは、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] **set SelectMemoryRAS**	サーバに対するメモリの Reliability, Availability, and Serviceability（RAS）の設定方法。 次のいずれかになります。 • 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]：システムは、DIMM に障害が発生した場合に使用するためのメモリを予約します。 障害が発生した場合、サーバは DIMM をオフラインにして、予約済みのメモリと置き換えます。 このオプションは、ミラーリングよりも冗長性が低くなりますが、サーバで実行するプログラムに使用できるメモリの量が多くなります。

名前	説明
[NUMA Optimized] **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] **set SparingMode**	CIMC で使用される予備設定モード。 次のいずれかになります。 • Rank_Sparing：ランク レベルで予備メモリが割り当てられます。 • [DIMM Sparing]：DIMM レベルで予備メモリが割り当てられます。 （注） このオプションは、set SelectMemoryRAS が [Sparing] に設定されている場合にのみ使用されます。
[Mirroring Mode] **set MirroringMode**	ミラーリングは Integrated Memory Controller（IMC）全体でサポートされ、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ます。 次のいずれかになります。 • [Intersocket]：各 IMC は 2 つのソケット全体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、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] **set PatrolScrub**	システムがサーバ上のメモリの未使用部分でも単一ビット メモリ エラーをアクティブに探して訂正するかどうか。 次のいずれかになります。 • [Disabled]：CPU がメモリ アドレスの読み取りまたは書き込みを行うときのみ、システムはメモリの ECC エラーをチェックします。 • [Enabled]：システムは定期的にメモリを読み書きして ECC エラーを探します。 エラーが見つかると、システムは修正を試みます。 このオプションにより、単一ビット エラーは複数ビット エラーになる前に修正される場合がありますが、パトロール スクラブの実行時にパフォーマンスが低下する場合もあります。
[Patrol Scrub Interval] **set PatrolScrubDuration**	各パトロール スクラブによるメモリ アクセスの時間間隔を制御します。 小さくすると、メモリのスクラブ頻度が高くなりますが、必要なメモリ帯域幅も多くなります。 5 ～ 23 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] **set CKELowPolicy**	DIMM の省電力モード ポリシーを制御します。 次のいずれかになります。 • [Disabled]：DIMM は省電力モードに入りません。 • [Slow]：DIMM は省電力モードに入ることができますが、要件が厳しくなります。 したがって、DIMM が省電力モードに入る頻度は低くなります。 • [Fast]：DIMM はできる限り頻繁に省電力モードに入ります。 • [Auto]：BIOS は DIMM の構成に基づいて DIMM が省電力モードに入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] **set Serial-PortA**	シリアル ポート A がイネーブルかディセーブルか。 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] **set MakeUSBDeviceNonBootable**	サーバが 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]：サーバは USB デバイスからブートできます。 • [Enabled]：サーバは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] **set MemoryMappedIOAbove4GB**	64 ビット PCI デバイスの 4 GB 以上のアドレス空間に対するメモリ マップド I/O をイネーブルにするか、ディセーブルにするか。 レガシーなオプション ROM は 4 GB を超えるアドレスにアクセスできません。 PCI デバイスが 64 ビット対応でも、レガシーなオプション ROM を使用する場合は、この設定をイネーブルにしても正しく機能しない場合があります。 次のいずれかになります。 • [Disabled]：サーバでは 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングしません。 • [Enabled]：サーバで 64 ビット PCI デバイスの I/O を 4 GB 以上のアドレス空間にマッピングします。

名前	説明
[Onboard NIC *n* ROM] **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] **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 を使用できません。 • [Enabled]：PCIe オプション ROM を使用できます。
[PCIe Slot *n* ROM] **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* を使用できません。 • [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] **set AssertNMIOnSERR**	システム エラー（SERR）の発生時に、BIOS がマスク不能割り込み（NMI）を生成し、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 は NMI を生成することもエラーをログに記録することもしません。 • [Enabled]：SERR の発生時に、BIOS は NMI を生成し、エラーをログに記録します。 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] **set AssertNMIOnPERR**	プロセッサ バス パリティ エラー（PERR）の発生時に、BIOS がマスク不能割り込み（NMI）を生成し、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 は NMI を生成することもエラーをログに記録することもしません。 • [Enabled]：PERR の発生時に、BIOS は 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 をイネーブルにする必要があります。
[Console Redirection] **set ConsoleRedir**	POST および BIOS のブート中に、シリアル ポートをコンソール リダイレクションに使用できるようにします。 BIOS のブートが完了し、オペレーティング システムがサーバを担当すると、コンソール リダイレクションは関連がなくなり、無効になります。 次のいずれかになります。 • [Disabled]：POST 中にコンソール リダイレクションは発生しません。 • Serial_Port_A：POST 中のコンソール リダイレクション用にシリアル ポート A を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場合は、POST 中に表示される Quiet Boot のロゴ画面もディセーブルにします。
[Flow Control] **set FlowCtrl**	フロー制御にハンドシェイク プロトコルを使用するかどうか。 送信要求/クリア ツー センド（RTS/CTS）を使用すると、隠れた端末問題が原因で発生する可能性があるフレーム コリジョンを減らすことができます。 次のいずれかになります。 • [None]：フロー制御は使用されません。 • [RTS-CTS]：RTS/CTS がフロー制御に使用されます。 （注） この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。

名前	説明
[Baud Rate] **set BaudRate**	シリアル ポートの伝送速度として使用されるボー レート。 [Console Redirection] をディセーブルにした場合は、このオプションを使用できません。 次のいずれかになります。 • [9.6k]：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 アプリケーション上の設定と一致している必要があります。
[Terminal Type] **set TerminalType**	コンソール リダイレクションに使用される文字フォーマットのタイプ。 次のいずれかになります。 • [PC-ANSI]：PC-ANSI 端末フォントが使用されます。 • [VT100]：サポートされている vt100 ビデオ端末とその文字セットが使用されます。 • [VT100-PLUS]：サポートされている vt100-plus ビデオ端末とその文字セットが使用されます。 • [VT-UTF8]：UTF-8 文字セットのビデオ端末が使用されます。 （注） この設定は、リモート ターミナル アプリケーション上の設定と一致している必要があります。

名前	説明
[OS Boot Watchdog Timer Timeout] **set OSBootWatchdogTimerTimeOut**	BIOS でウォッチドッグ タイマーの設定に使用されるタイムアウト値。 次のいずれかになります。 • 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：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：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：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] **set OSBootWatchdogTimerPolicy**	ウォッチドッグ タイマーが切れた場合にシステムで実行されるアクション。 次のいずれかになります。 • 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] **set LegacyOSRedir**	シリアル ポートでレガシーなオペレーティング システム（DOS など）からのリダイレクションを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 リダイレクションがイネーブルになっているシリアル ポートは、レガシーなオペレーティング システムから認識されません。 • [Enabled]：コンソール リダイレクションがイネーブルになっているシリアル ポートは、レガシーなオペレーティング システムから認識できます。

名前	説明
[OS Boot Watchdog Timer] **set OSBootWatchdogTimer**	BIOS が指定されたタイムアウト値でウォッチドッグ タイマーをプログラムするかどうか。次のいずれかになります。 • [Disabled]：サーバのブートにかかる時間をトラッキングするためにウォッチドッグ タイマーは使用されません。 • [Enabled]：サーバのブートにかかる時間をウォッチドッグ タイマーでトラッキングします。 サーバが **set OSBootWatchdogTimerTimeout** コマンドで指定された時間内にブートしない場合、CIMC はエラーをログに記録し、**set OSBootWatchdogTimerPolicy** コマンドで指定されたアクションを実行します。

索 引

A

Active Directory 63, 64, 66
- CIMC の設定 64
- グループの設定 66

B

BIOS 151
- TFTP サーバからのインストール 151

bios 164
- 破損の回復 164

BIOS ステータス 30
- 表示 30

BIOS 設定 16, 31, 32, 33, 34
- 高度 32
- サーバ管理 33
- サーバのブート順 16
- 主要 31
- デフォルトの復元 34

BIOS パラメータ 169, 170, 183, 186, 187, 198, 202, 213, 217, 218, 228
- 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 202
- C460 の高度なパラメータ 218
- C460 のサーバ管理パラメータ 228
- 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 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 202

C460 サーバ 217, 218, 228
- 高度な BIOS パラメータ 218
- サーバ管理 BIOS パラメータ 228
- 主要な BIOS パラメータ 217

CIMC 36, 147, 148, 149, 150, 153, 154, 156, 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
  - TFTP サーバからのインストール 149
  - アクティブ化 150
  - 概要 147
  - シスコからの取得 148
- プロパティの表示 36
- ログしきい値の設定 154
- ログのクリア 154
- ログの送信 156
- ログの表示 153

CIMC CLI 4

CIMC の概要 2

CPU プロパティ 36

D

date 36
　設定 36

F

FEX 106, 107
　説明 106
　プロパティの表示 107
FIP モード 81
　イネーブル化 81
Flexible Flash 26, 28, 29, 40
　からのブート 28
　説明 26
　プロパティの設定 26
　プロパティの表示 40
　リセット 29

H

HTTP プロパティ 119

I

IPMI over LAN 122
　説明 122
IPMI over LAN プロパティ 122
IPv4 プロパティ 74
IP ブロッキング 77

K

KVM 54, 55
　イネーブル化 54, 55
　設定 55
　ディセーブル化 54
KVM コンソール 11, 53
KVM のイネーブル化 54, 55
KVM のディセーブル化 54

L

LDAP。参照先： Active Directory
LOM ポート 44
　プロパティの表示 44

M

MAC アドレス 44
　LOM ポート 44

N

NIC プロパティ 72
NIV モード 81
　イネーブル化 81

O

OS のインストール 11, 13
　PXE 13
　方法 11

P

PCI アダプタ 44
　プロパティの表示 44
PXE インストール 12

S

Serial over LAN 57, 58, 59
　起動 59
　設定 58
SNMP 124, 125, 126, 127, 141, 142
　SNMPv3 ユーザの設定 127
　テスト メッセージの送信 126, 142
　トラップ設定の指定 125, 141
　プロパティの設定 124
SSH プロパティ 120
syslog 156
　CIMC ログの送信 156

T

Telnet 4

time 36
設定 36

V

vHBA 82, 83, 84, 89, 90, 91, 92, 93, 94, 95, 96
永続的なバインディング 94
永続的なバインディングのイネーブル化 94
永続的なバインディングの再構築 96
永続的なバインディングのディセーブル化 95
管理のガイドライン 82
削除 90
作成 89
ブート テーブル エントリの削除 91, 93
ブート テーブル 91
ブート テーブル エントリの作成 92
プロパティの表示 83
プロパティの変更 84
VLAN プロパティ 76
VM FEX 106, 107
説明 106
プロパティの表示 107
vNIC 96, 97, 98, 105, 106
管理のガイドライン 96
削除 106
作成 105
プロパティの表示 97
プロパティの変更 98

X

XML API 121
イネーブル化 121
説明 121

Y

YAML 9

あ

アダプタ 44, 79, 80, 81, 113, 114, 115, 117
PCI 44
概要 79
設定のインポート 114
アダプタ (続き)
設定のエクスポート 113
デフォルト設定の復元 114
ネットワーク 80
ファームウェア 115
ファームウェアのアクティブ化 117
ファームウェアのインストール 115
プロパティの設定 81
プロパティの表示 80

い

イベント 138
プラットフォーム 138
アラートのイネーブル化 138
アラートのディセーブル化 138
イベント フィルタ、プラットフォーム 137, 139
概要 137
設定 139
イベント ログ、システム 157, 158
クリア 158
表示 157
インポート 167
CIMC 設定 167

え

永続的なバインディング 94, 95, 96
イネーブル化 94
再構築 96
説明 94
ディセーブル化 95
エクスポート 166
CIMC 設定 166

お

温度センサー 49

か

仮想 KVM 54, 55
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 74

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 119, 120, 122
HTTP プロパティ 119
IPMI over LAN プロパティ 122
SSH プロパティ 120

さ

サーバ 35
プロパティの表示 35
サーバ概要 1
サーバ管理 15, 16, 18, 19, 20, 21
サーバ電源の再投入 21
サーバのシャットダウン 19
サーバの電源オフ 20
サーバの電源投入 19
サーバのブート順 16
サーバのリセット 18
ロケータ LED の切り替え 15
サーバ管理 BIOS パラメータ 183, 198, 213, 228
C200 および C210 サーバ 183
C250 サーバ 198
C260 サーバ 213
C460 サーバ 228
サーバ証明書のアップロード 136
サーバ ソフトウェア 2
サーバ電源の再投入 21
サーバの NIC 71
サーバのシャットダウン 19
サーバの電源オフ 20
サーバの電源投入 19
サーバのリセット 18

し

自己署名証明書 133
システム イベント ログ 157, 158
クリア 158
表示 157
主要な BIOS パラメータ 169, 186, 202, 217
C200 および C210 サーバ 169
C250 サーバ 186
C260 サーバ 202
C460 サーバ 217
障害 47
サマリーの表示 47
障害サマリー 47
表示 47
証明書管理 136
証明書のアップロード 136

す

ストレージ センサー 51
表示 51
ストレージのプロパティ 39, 41, 43
アダプタのプロパティの表示 39
仮想ドライブのプロパティの表示 43
物理ドライブのプロパティの表示 41

せ

設定 166, 167
インポート 167
エクスポート 166
バックアップ 166
センサー 48, 49, 50
temperature 49
電圧 50
電源装置 48
電流 50
ファン 48

て

テクニカル サポート データ 161
エクスポート 161
電圧センサー 50

電源センサー 48
電源のプロパティ 38
電流センサー 50
電力制限ポリシー 23
　概要 23
　設定 23
電力統計情報 21
　表示 21
電力復元ポリシー 24

ね

ネットワーク アダプタ 80
　プロパティの表示 80
ネットワーク セキュリティ 77
ネットワーク プロパティ 72, 74, 76
　IPv4 プロパティ 74
　NIC プロパティ 72
　VLAN プロパティ 76
　共通プロパティ 74

は

破損した BIOS のリカバリ 164
バックアップ 166
　CIMC 設定 166

ふ

ファームウェア 147, 148, 149, 150
　TFTP サーバからのインストール 149
　アクティブ化 150
　概要 147
　シスコからの取得 148
ファン センサー 48
ブート順 16, 17
　概要 16
　設定 16
　表示 17
ブート テーブル 91, 92, 93
　エントリの削除 91, 93
ブート テーブル (続き)
　エントリの作成 92
　説明 91
プラットフォーム イベント 138, 143
　アラートのイネーブル化 138
　アラートのディセーブル化 138
　トラップの解釈 143
プラットフォーム イベント フィルタ 137, 139
　概要 137
　設定 139
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 37

ゆ

ユーザ管理 61, 64, 68
　Active Directory 64
　終了、ユーザ セッション 68
　ユーザ セッションの表示 68
　ローカル ユーザ 61
ユーザ セッション 68
　終了 68
　表示 68

り

リモート プレゼンス 54, 55, 56, 58, 59
　Serial over LAN の起動 59
　Serial over LAN の設定 58
　仮想 KVM 54, 55
　仮想メディア 56

ろ

ローカル ユーザ 61
ロケータ LED の切り替え 15