Cisco UCS E シリーズ サーバ Integrated Management Controller の CLI 設定ガイド リリース 2.x

初版：2013 年 08 月 09 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-28562-01-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。

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号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、ネットワーク トポロジ図、およびその他の図は、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および電話番号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。

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)

© 2013 Cisco Systems, Inc. All rights reserved.

目 次

はじめに ix

対象読者 ix

マニュアルの構成 ix

表記法 xi

新機能および変更された機能に関する情報 xii

関連資料 xiii

マニュアルに関するフィードバック xiv

概要 1

Cisco UCS E シリーズ サーバの概要 1

サーバ ソフトウェア 1

CIMC の概要 2

CIMC CLI 3

コマンド モード 4

コマンド モード表 5

コマンドの完了または終了 7

コマンド履歴 7

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 8

CLI に関するオンラインヘルプ 9

サーバのオペレーティング システムまたはハイパーバイザのインストール 11

オペレーティング システムまたはハイパーバイザのインストール方法 11

KVM コンソール 12

KVM コンソールを使用したオペレーティング システムまたはハイパーバイザのインストール 12

PXE インストール サーバ 12

PXE インストール サーバを使用したオペレーティング システムまたはハイパーバイザのインストール 13
ホスト イメージ マッピング 13
ホスト イメージのマッピング 14
Microsoft Windows Server 用のドライバのインストール 16
ホスト イメージのマッピング解除 16
ホスト イメージの削除 17
カスタマイズされた VMware vSphere Hypervisor イメージのダウンロード 18
サーバの管理 19
サーバのブート順の設定 19
サーバのリセット 21
サーバのシャットダウン 22
Cisco IOS CLI 設定変更のロック 22
Cisco IOS CLI 設定変更のロック解除 23
サーバの電源管理 24
サーバの電源投入 24
サーバの電源オフ 25
サーバ電源の再投入 26
サーバの前面パネルの電源ボタンのロック 26
サーバの前面パネルの電源ボタンのロック解除 27
BIOS の設定 29
BIOS ステータスの表示 29
BIOS の詳細設定 29
サーバ管理 BIOS の設定 30
BIOS CMOS のクリア 31
BIOS パスワードのクリア 32
BIOS デフォルトの復元 32
サーバ BIOS 設定 33
RAID の管理 45
RAID オプション 45
RAID の設定 49
RAID 設定の削除 52

物理ドライブの状態の変更 53
物理ドライブの再構築 54
物理ドライブの内容の削除 55
ストレージ コントローラ上での自動再構築のイネーブル化 57
仮想ドライブの削除 58
仮想ドライブの整合性検査の実行 58
仮想ドライブの再構築のオプション 60
仮想ドライブの再構築 63
ディスク ドライブのブート可能化 64
サーバのプロパティの表示 67
サーバのプロパティの表示 67
実際のブート順の表示 68
CIMC 情報の表示 69
CPU のプロパティの表示 69
メモリのプロパティの表示 70
電源のプロパティの表示 71
ストレージのプロパティの表示 71
ストレージ アダプタのプロパティの表示 71
物理ドライブのプロパティの表示 73
仮想ドライブのプロパティの表示 74
PCI アダプタのプロパティの表示 75
電源ポリシーの統計情報の表示 76
ハード ドライブのプレゼンスの表示 76
インターフェイスの MAC アドレスの表示 77
CIMC ネットワーク接続ステータスの表示 78
サーバのセンサーの表示 79
障害サマリーの表示 79
温度センサーの表示 80
電圧センサーの表示 80
LED センサーの表示 81
ストレージ センサーの表示 82
リモート プレゼンスの管理 83

仮想 KVM の管理 83
KVM コンソール 83
仮想 KVM の設定 84
仮想 KVM のイネーブル化 85
仮想 KVM のディセーブル化 85
仮想メディアの設定 86
Serial over LAN の管理 87
Serial over LAN 87
Serial over LAN に関するガイドラインおよび制約事項 87
Serial over LAN の設定 88
Serial Over LAN の起動 89
ユーザ アカウントの管理 91
ローカル ユーザの設定 91
Active Directory 92
Active Directory サーバの設定 93
CIMC での Active Directory の設定 94
ユーザ セッションの表示 96
ユーザ セッションの終了 96
ネットワーク関連の設定 99
CIMC NIC の設定 99
CIMC NIC 99
CIMC NIC の設定 100
共通プロパティの設定 102
IPv4 の設定 102
サーバ VLAN の設定 104
ネットワーク セキュリティの設定 105
ネットワーク セキュリティ 105
ネットワーク セキュリティの設定 105
コミュニケーション サービスの設定 107
HTTP の設定 107
SSH の設定 108
XML API の設定 109
CIMC の XML API 109

XML API のイネーブル化 109
IPMI の設定 110
IPMI over LAN 110
IPMI over LAN の設定 110
SNMP の設定 112
SNMP 112
SNMP プロパティの設定 112
SNMP トラップ設定の指定 113
テスト SNMP トラップ メッセージの送信 114
SNMPv3 ユーザの設定 115
証明書の管理 119
サーバ証明書の管理 119
証明書署名要求の生成 120
自己署名証明書の作成 121
サーバ証明書のアップロード 123
プラットフォーム イベント フィルタの設定 125
プラットフォーム イベント フィルタ 125
プラットフォーム イベント アラートのイネーブル化 126
プラットフォーム イベント アラートのディセーブル化 126
プラットフォーム イベント フィルタの設定 127
プラットフォーム イベント トラップの解釈 128
ファームウェアの管理 131
ファームウェアの概要 131
Cisco Systems からファームウェアを取得するためのオプション 132
シスコからのソフトウェアの取得 132
リモート サーバからの CIMC ファームウェアのインストール 134
インストールした CIMC ファームウェアのアクティブ化 135
TFTP サーバからの BIOS ファームウェアのインストール 137
ログの表示 139
CIMC ログ 139
CIMC ログの表示 139
CIMC ログのクリア 140
CIMC ログしきい値の設定 140

リモート サーバへの CIMC ログの送信 142
System Event Log 143
システム イベント ログの表示 143
システム イベント ログのクリア 144
サーバ ユーティリティ 145
リモート サーバへのテクニカル サポート データのエクスポート 145
CIMC の再起動 147
CIMC の出荷時デフォルトへのリセット 148
CIMC 設定のエクスポートとインポート 149
CIMC 設定のエクスポートとインポート 149
CIMC 設定のエクスポート 149
CIMC 設定のインポート 150
診断テスト 153
診断テストの概要 153
ホストへの診断イメージのマッピング 154
診断テストの実行 155

はじめに

この章は、次の項で構成されています。

- 対象読者，ix ページ
- マニュアルの構成，ix ページ
- 表記法，xi ページ
- 新機能および変更された機能に関する情報，xii ページ
- 関連資料，xiii ページ
- マニュアルに関するフィードバック，xiv ページ

対象読者

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

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

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 E-Series Servers と CIMC CLI について説明します。

章	タイトル	説明
第 2 章	サーバのオペレーティング システムのインストール	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	サーバの起動デバイス順序の設定方法、サーバの電源の管理方法、電力使用ポリシーの設定方法、および BIOS の設定方法について説明します。
第 4 章	RAID の管理	RAID を設定および管理する方法を説明します。
第 5 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、PCI アダプタ、および LOM プロパティを表示する方法を説明します。
第 6 章	サーバのセンサーの表示	障害、温度、電圧、およびストレージのセンサーの表示方法を説明します。
第 7 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 8 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 9 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 10 章	コミュニケーション サービスの設定	HTTP、SSH、IPMI、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を説明します。
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。

章	タイトル	説明
第 15 章	サーバ ユーティリティ	サポート データのエクスポート方法、サーバ設定のエクスポート方法とインポート方法、サーバ設定を出荷時デフォルトにリセットする方法、管理インターフェイスのリブート方法を説明します。
第 16 章	診断テスト	診断テストの実行方法を説明します。

表記法

このマニュアルでは、次の表記法を使用しています。

表記法	用途
太字フォント	コマンド、キーワード、およびユーザが入力したテキストは、**太字**フォントで示しています。
イタリック体フォント	ドキュメント名、新規用語または強調する用語、値を指定するための引数は、イタリック体フォントで示しています。
`courier` フォント	システムが表示するターミナル セッションおよび情報は、`courier` フォントで示しています。
[ ]	角カッコの中の要素は、省略可能です。
{x | y | z}	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。

表記法	用途
! #	コードの先頭に感嘆符（!）またはポンド記号（#）がある場合には、コメント行であることを示します。

（注） 「注釈」です。

ヒント 「問題解決に役立つ情報」です。

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

ワンポイント アドバイス 時間を節約する方法です。 ここに紹介している方法で作業を行うと、時間を短縮できます。

警告 「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。

新機能および変更された機能に関する情報

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。

表 *1*：*Cisco Integrated Management Controller* ソフトウェア リリース *2.0* の新機能と重要な動作の変更

機能	説明	参照先
ブート オプション	デバイス カテゴリ内の特定のデバイスからのサーバの起動のサポートが追加されました。	サーバの管理，（19 ページ）
リンクの状態	CIMC ネットワーク接続ステータスの表示のサポートが追加されました。	サーバのプロパティの表示，（67 ページ）
LOM プロパティ	システム定義のインターフェイス名と、各インターフェイスに割り当てられている MAC アドレスの表示のサポートが追加されました。	サーバのプロパティの表示，（67 ページ）

機能	説明	参照先
RAID	RAID 機能が強化されました。 仮想ドライブを削除し、物理ドライブの内容を削除する CLI が追加されました。	RAID の管理, （45 ページ）
SNMP	SNMPv3 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, （107 ページ）
テクニカル サポート	リモート サーバへのテクニカル サポート情報のエクスポートのサポートが追加されました。	サーバ ユーティリティ, （145 ページ）
XML API	XML API による CIMC 制御の追加サポート。	コミュニケーション サービスの設定, （107 ページ）

関連資料

『http://www.cisco.com/en/US/docs/unified_computing/ucs/e/1.0/roadmap/e_series_road_map.html』には、すべての E シリーズ サーバ ドキュメントへのリンクが含まれています。

- 『*Release Notes for Cisco UCS E-Series Servers*』
- 『*Getting Started Guide for Cisco UCS E-Series Servers*』
- 『*Hardware Installation Guide for Cisco UCS E-Series Servers*』
- 『*Cisco Network Modules, Server Modules, and Interface Cards Regulatory Compliance and Safety Information*』
- 『*Host Upgrade Utility Guide for Cisco UCS E-Series Servers*』
- 『*GUI Configuration Guide for Cisco UCS E-Series Servers Integrated Management Controller*』
- 『*CLI Configuration Guide for Cisco UCS E-Series Servers Integrated Management Controller*』
- 『*CIMC XML API Programmer's Guide for Cisco UCS E-Series Servers*』
- 『*Troubleshooting Guide for Cisco UCS E-Series Servers*』
- 『*Open Source Used in Cisco UCS E-Series Servers*』

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

この章は、次の内容で構成されています。

- Cisco UCS E シリーズ サーバの概要，1 ページ
- サーバ ソフトウェア，1 ページ
- CIMC の概要，2 ページ
- CIMC CLI，3 ページ

Cisco UCS E シリーズ サーバの概要

Cisco UCS E-Series Servers（E シリーズ サーバ）は、次世代の Cisco UCS Express サーバです。 E シリーズ サーバは、サイズ効率、重量効率、電力効率に優れたブレード サーバのファミリであり、Generation 2 Cisco Integrated Services Router（ISR G2）および Cisco 4451-X サービス統合型ルータ（Cisco ISR 4451-X）に収容されます。 これらのサーバは、オペレーティング システム（Microsoft Windows や Linux など）上でベアメタルとして、あるいはハイパーバイザ（VMware vSphere Hypervisor™、Microsoft Hyper-V、Citrix XenServer など）上で仮想マシンとして導入される、ブランチオフィス アプリケーション向けの汎用コンピューティング プラットフォームを提供します。

（注） サポートされる E シリーズ サーバと、ISR ごとにインストール可能な E シリーズ サーバの最大数については、『*Release Notes for Cisco UCS E-Series Servers*』の「Hardware Requirements」の項を参照してください。

サーバ ソフトウェア

E シリーズ サーバには、3 つの主要なソフトウェア システムが必要です。

- CIMC ファームウェア

- BIOS ファームウェア
- オペレーティング システムまたはハイパーバイザ

CIMC ファームウェア

Cisco Integrated Management Controller（CIMC）は、E シリーズ サーバの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。

CIMC は、E シリーズ サーバ用の管理サービスです。 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。

BIOS ファームウェア

BIOS は、システム内のハードウェアを初期化し、ブート可能なデバイスを検出し、それらを指定された順序でブートします。 オペレーティング システムを起動したり、オペレーティング システムが使用するハードウェアを設定したりします。 使いやすい BIOS 管理機能により、ハードウェアを操作したり、使用したりできます。 他にも BIOS では、システムを設定したり、ファームウェアを管理したり、BIOS エラー レポートを作成したりすることもできます。

システムには、現行バージョンの BIOS ファームウェアが付属しています。 BIOS 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。

オペレーティング システムまたはハイパーバイザ

メイン サーバ CPU は、オペレーティング システム（Microsoft Windows や Linux など）上またはハイパーバイザ上で動作します。 Microsoft Windows Server または VMware vSphere Hypervisor™ がプレインストールされている E シリーズ サーバ を購入することも、独自のプラットフォームをインストールすることもできます。

（注） E シリーズ サーバでテストされたプラットフォームについては、『『*Release Notes for Cisco UCS E-Series Servers*』』の「Software Requirements」の項を参照してください。

CIMC の概要

Cisco Integrated Management Controller（CIMC）は、E 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。 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。

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
- サーバのブート順を設定する

- RAID レベルを管理する
- 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、SNMP などのコミュニケーション サービスを設定する
- 証明書を管理する
- プラットフォーム イベント フィルタを設定する
- CIMC ファームウェアを更新する
- BIOS ファームウェアを更新する
- 内部リポジトリからホスト イメージをインストールする
- 障害、アラーム、およびサーバのステータスをモニタする
- サーバ障害の発生時にテクニカル サポート データを収集する

ほとんどすべてのタスクは、GUI インターフェイスと CLI 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、次の操作は実行できません。

- 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 出力を生成する

CIMC CLI

CIMC CLI は、E 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。 CIMC CLI は、次の方法で起動できます。

- シリアル ポートを使用する。
- SSH を介してネットワーク上で。
- **hw-module subslot** *slot/port* **session imc** コマンドを使用してルータから。

CLI ユーザには、admin、user（コントロールはできるが設定はできない）、および read-only のいずれかのロールが与えられます。

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 #
dimm-summary	シャーシ モードから **scope dimm-summary** *index* コマンド	/chassis/dimm-summary #
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** *drive-number* コマンド	/chassis/storageadapter /physical-drive #
virtual-drive	storageadapter モードから **scope virtual-drive** *drive-number* コマンド	/chassis/storageadapter /virtual-drive #
cimc	EXEC モードから **scope cimc** コマンド	/cimc #
import-export		

モード名	アクセスするコマンド	モード プロンプト
	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 #
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 #
power-cap	EXEC モードから **scope power-cap** コマンド	/power-cap #
remote-install	EXEC モードから **scope remote-install** コマンド	/remote-install #
sel	EXEC モードから **scope sel** コマンド	/sel #

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

コマンドの完了または終了

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。

スコープ内にある場合、**exit** コマンドで 1 レベル上位に移動できます。 たとえばスコープが **/chassis/dimm-summary** のときに **exit** を入力した場合、スコープは 1 レベル上位の **/chassis** まで移動します。

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 kvm
Server /kvm # set enabled yes
Server /kvm *# commit
Server /kvm #
```

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。

注意 同じスコープの中で行った変更をコミットするには、**commit** コマンドを使用しなければなりません。 **commit** コマンドを使用して、別のスコープで行った変更の送信を試みると、エラーが返されます。これらの変更は再実行し、再コミットする必要があります。

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。

出力情報を **detail** コマンドで表示する方法に応じて、次のコマンドのいずれかを使用します。

- **set cli output default**：見やすいデフォルト形式。 コマンド出力は、コンパクトな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
```

```
Server /chassis #
```

- **set cli output yaml**：スクリプトによって簡単に解析できる YAML 形式。 コマンド出力は、定義された文字列で区切られた YAML Ain't Markup Language（YAML）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

...

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。

CLI に関するオンラインヘルプ

疑問符（**?**）文字を入力すれば、いつでも コマンド構文の現在の状態で使用可能なオプションが表示されます。 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

サーバのオペレーティング システムまたはハイパーバイザのインストール

この章は、次の内容で構成されています。

- オペレーティング システムまたはハイパーバイザのインストール方法，11 ページ
- KVM コンソール，12 ページ
- PXE インストール サーバ，12 ページ
- ホスト イメージ マッピング，13 ページ

オペレーティングシステムまたはハイパーバイザのインストール方法

E シリーズ サーバでは、複数種類のオペレーティング システムとハイパーバイザがサポートされています。 インストールされるプラットフォームに関係なく、次のいずれかの方法で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
- ホスト イメージ マッピング

注意 仮想ドライブのマッピングには、1 つの方法だけを使用する必要があります。 たとえば、KVM コンソールまたはホスト イメージ マッピング方式を使用します。 複数の方法を組み合わせて使用すると、サーバが未定義の状態になります。

KVM コンソール

KVM コンソールは、CIMC からアクセス可能なインターフェイスであり、サーバへのキーボード、ビデオ、マウス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

KVM コンソールを使用して、サーバにオペレーティング システムまたはハイパーバイザをインストールし、次の作業を行うことができます。

- 起動中に F2 を押して、BIOS セットアップ メニューにアクセスします。
- 起動中に F8 を押して、CIMC 設定ユーティリティにアクセスします。
- 起動中に Ctrl キーと H キーを押して WebBIOS にアクセスし、RAID を設定します。

KVMコンソールを使用したオペレーティングシステムまたはハイパーバイザのインストール

KVM コンソールは GUI を介してのみ動作するため、CLI を使用してオペレーティング システムまたはハイパーバイザ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プラットフォームをインストールするには、『*GUI Configuration Guide for Cisco UCS E-Series Servers*』のセクション「Installing an Operating System or Hypervisor Using the KVM Console」の説明に従ってください。

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オペレーティング システムまたはハイパーバイザ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、サーバにオペレーティング システムまたはハイパーバイザ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、オペレーティング システムまたはハイパーバイザ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、プラットフォーム、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、多数のサーバにプラットフォーム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オペレーティングシステムまたはハイパーバイザのインストール

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。

（注） VMware vSphere Hypervisor™ では、カスタマイズされたイメージが必要です。 カスタマイズされたイメージをダウンロードするには、カスタマイズされた VMware vSphere Hypervisor イメージのダウンロード, （18 ページ）を参照してください。

手順

ステップ 1 ブート順を [PXE] 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オペレーティング システムまたはハイパーバイザ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

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。

ホスト イメージ マッピング

ホスト イメージ マッピング機能を使用すると、ホスト イメージのダウンロード、マッピング、マッピング解除、または削除を行うことができます。 リモートFTP またはHTTP サーバから CIMC

内部リポジトリに、Microsoft Windows、Linux、または VMware などのホスト イメージをダウンロードした後、そのイメージを E シリーズ サーバ内の USB コントローラの仮想ドライブにマップします。イメージをマップした後は、イメージをマウントした仮想ドライブが最初のブートデバイスになるようにブート順序を設定してから、サーバをリブートします。 ホスト イメージのファイル拡張子は必ず、.iso または .img になります。

また、ホストイメージマッピング機能により、診断イメージをダウンロードし、マウントできます。 診断イメージのファイル拡張子は必ず .diag になります。

ホスト イメージのマッピング

はじめる前に

- admin 権限を持つユーザとして CIMC にログインします。
- 適切なサードパーティからホスト イメージ ファイルを取得します。

（注） VMware vSphere Hypervisor™ では、カスタマイズされたイメージが必要です。 カスタマイズされたイメージをダウンロードするには、カスタマイズされた VMware vSphere Hypervisor イメージのダウンロード, （18 ページ）を参照してください。

（注） アップデートがすでに処理中であるときにイメージ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 remote-install**	remote install コマンド モードを開始します。
ステップ 2	Server /remote-install # **download-image** {**ftp** | **ftps** | **http** | **https**} *server-ip-address path / filename* [**username** *username* **password** *password*]	指定したリモート サーバから CIMC 内部リポジトリにイメージをダウンロードします。 ホスト イメージのファイル拡張子は必ず .iso になります。 リモート サーバには、FTP、FTPS、HTTP、または HTTPS サーバを指定できます。 リモート サーバでユーザ認証が必要な場合は、リモート サーバのユーザ名とパスワードを追加する必要があります。 （注） イメージ ファイルがサイズ制限を超えると、エラー メッセージが表示されます。
ステップ 3	（任意）Server /remote-install # **show detail**	イメージ ダウンロードのステータスを表示します。

	コマンドまたはアクション	目的
ステップ 4	Server /remote-install # **map-image**	USB コントローラの仮想ドライブにイメージをマウントします。仮想ドライブには、次のいずれかを使用できます。 • HDD：ハード ディスク ドライブ • FDD：フロッピー ディスク ドライブ • CDROM：ブート可能 CD-ROM
ステップ 5	（任意）Server /remote-install # **show detail**	ホスト イメージ マッピングのステータスを表示します。

次に、ホストのイメージをマッピングする例を示します。

```
Server# scope remote-install
Server /remote-install # download-image ftp 10.20.34.56 pub/hostimage.iso
---
Server /remote-install # show detail
Host Image Info:
  Name: HostImage.iso
  Size: 6626848
  Last Modified Time: Fri, 12 Aug 2011 21:13:27 GMT
  Host Image Status: Download Successful!!
Server /remote-install # map-image
---
status: ok
---
Server /remote-install # show detail
Host Image Info:
  Name: HostImage.iso
  Size: 6626848
  Last Modified Time: Fri, 12 Aug 2011 21:13:27 GMT
  Host Image Status: Image mapped successfully!!
```

次の作業

1. イメージがインストールされている仮想ドライブが最初にブートされるデバイスになるように、ブート順を設定します。 サーバのブート順の設定，（19 ページ）を参照してください。
2. サーバをリブートします。イメージにアンサーファイルが含まれている場合は、オペレーティング システムのインストールは自動化され、イメージがインストールされます。 それ以外の場合は、インストール ウィザードが表示されます。 ウィザードの手順に従って、イメージをインストールします。
3. オペレーティング システムまたはハイパーバイザをインストールした後にディスク ドライブが表示されない場合は、ドライバをインストールする必要があります。 Microsoft Windows Server へのドライバのインストール方法については、Microsoft Windows Server 用のドライバのインストール，（16 ページ）を参照してください。
4. インストールが完了したら、仮想メディアのブート順を元の設定にリセットします。

Microsoft Windows Server 用のドライバのインストール

（注） E シリーズ サーバ オプション 1（オペレーティング システムやハイパーバイザが事前にインストールされていない E シリーズ サーバ）を購入し、Microsoft Windows Server を自分でインストールした場合は、ドライバをインストールする必要があります。

Microsoft Windows オペレーティング システムでは、3 種類のドライバをインストールする必要があります。

- Windows 2008 R2 用のオンボード ネットワーク ドライバ
- Windows 2008 R2 用の LSI ドライバ（オンボード ハードウェア RAID コントローラ）
- Windows 2008 R2 用の Intel ドライバ

（注） Windows 2012 には、追加ドライバは不要です。

10 ギガビット アドオン カードを購入した場合は、Windows 2008 R2 用の 10G PCIe ネットワーク ドライバもインストールする必要があります。

手順

ステップ 1 ドライバを Cisco.com からダウンロードします。シスコからのソフトウェアの取得, （132 ページ）を参照してください。

ステップ 2 ドライバ ファイルを USB フラッシュ ドライブにコピーします。

ステップ 3 使用する Microsoft Windows Server をインストールします。
インストール プロセスの途中で、LSI ドライバを要求されます。

ステップ 4 USB フラッシュ ドライブを E シリーズ サーバの USB スロットに差し込み、LSI ドライバをインストールします。

ステップ 5 Microsoft Windows Server のインストールが完了したら、オンボード ネットワーク ドライバ（Broadcom）と Intel ドライバをインストールします。

ホスト イメージのマッピング解除

はじめる前に

admin 権限を持つユーザとして CIMC にログインします。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope remote-install**	remote install コマンド モードを開始します。
ステップ 2	Server /remote-install # **unmap-image**	USB コントローラの仮想ドライブからイメージをマウント解除します。
ステップ 3	Server /remote-install # **show detail**	（任意）ホスト イメージのマッピング解除のステータスを表示します。

次に、ホストのイメージのマッピングを解除する例を示します。

```
Server# scope remote-install
Server /remote-install # unmap-image
Server /remote-install # show detail
Host Image Info:
  Name: HostImage.iso
  Size: 6626848
  Last Modified Time: Fri, 12 Aug 2011 21:13:27 GMT
  Host Image Status: Image unmapped successfully!!
```

ホスト イメージの削除

はじめる前に

admin 権限を持つユーザとして CIMC にログインします。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope remote-install**	remote install モードを開始します。
ステップ 2	Server /remote-install # **delete-image**	CIMC 内部リポジトリからイメージを削除します。

次に、ホストのイメージを削除する例を示します。

```
Server# scope remote-install
Server /remote-install # delete-image
```

カスタマイズされた VMware vSphere Hypervisor イメージのダウンロード

手順

ステップ 1 https://my.vmware.com/web/vmware/login にアクセスします。
VMware ログイン ページが表示されます。

ステップ 2 自分の VMware クレデンシャルを入力し、[Log In] をクリックします。
VMware のアカウントがない場合は、[Register] をクリックして無料アカウントを作成します。

ステップ 3 [Support Requests] ペインの下で、[Knowledge Base] をクリックします。

ステップ 4 右上隅の [Search] フィールドに ESXi-5.0.0-623860-custom-Cisco-2.0.1.6.iso と入力し、[Search] をクリックします。

ステップ 5 [Search Results] から、[Download VMware View 5.1] をクリックして、カスタマイズされた VMware vSpere Hypervisor™ イメージをダウンロードします。

次の作業

VMware vSpere Hypervisor™ イメージをインストールします。インストール手順については、ホスト イメージのマッピングを参照してください。

第 3 章

サーバの管理

この章は、次の内容で構成されています。

- サーバのブート順の設定，19 ページ
- サーバのリセット，21 ページ
- サーバのシャットダウン，22 ページ
- Cisco IOS CLI 設定変更のロック，22 ページ
- Cisco IOS CLI 設定変更のロック解除，23 ページ
- サーバの電源管理，24 ページ
- BIOS の設定，29 ページ

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。

	コマンドまたはアクション	目的
ステップ 2	Server /bios # **set boot-order** *category:device1*[,*category:device2*[,*category:device3*[,*category:device4*[,*category:device5*]]]]	ブート デバイス オプションと順序を指定します。 （注） オプションでは、大文字と小文字は区別されません。 次の 1 つ以上を選択できます。 • cdrom：ブート可能な CD-ROM ◦ 仮想 CD • fdd：フロッピーディスク ドライブ ◦ 仮想フロッピー • hdd：ハードディスク ドライブ ◦ RAID ◦ Cypress ◦ 仮想 HiFD • pxe：PXE ブート ◦ GigEth0 ◦ GigEth1 ◦ GigEth2 ◦ GigEth3 • 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。
ステップ 4	（任意）Server /bios # **show detail**	サーバのブート順を表示します。

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 cdrom:Virtual-CD,hdd:raid,efi
To manage boot-order:
- Reboot server to have your boot-order settings take place
- Do not disable boot options via BIOS screens
```

```
- If a specified device type is not seen by the BIOS, it will be removed
  from the boot order configured on the BMC
- Your boot order sequence will be applied subject to the previous rule.
  The configured list will be appended by the additional device types
  seen by the BIOS
Server /bios *# commit
Server /bios #
Server /bios # show detail
BIOS:
    BIOS Version: "UCSES.1.5.0.1 (Build Date: 02/14/2013)"
    Boot Order: CDROM:Virtual-CD,HDD:RAID,EFI
    FW Update/Recovery Status: None, OK
    Active BIOS: main
```

サーバのリセット

はじめる前に

このタスクを実行するには、user または admin 権限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 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。 （注） • サーバ電源の再投入は、サーバの実際の電源ボタンを押して電源をオフにした後、電源をオンにする動作と同じです。 • 電源のハード リセットは、サーバの実際のリセット ボタンを押す動作と同じです。

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

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 chassis**	シャーシ モードを開始します。
ステップ 2	Server /chassis # **power shutdown**	確認プロンプトの後で、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
This operation will change the server's power state.
Do you want to continue?[y|N]y
```

Cisco IOS CLI 設定変更のロック

この手順を使用して、Cisco IOS CLI で設定変更が行われないようにします。

はじめる前に

このタスクを実行するには、user または admin 権限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 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 detail**	（任意）サーバのプロパティを表示します。これで、IOS ロックアウトの現在のステータス（ロックされているか、またはロック解除されているか）を判断できます。
ステップ 3	Server /chassis # **set ios-lockout locked**	Cisco IOS CLI を使用して設定変更が行われないようにします。

	コマンドまたはアクション	目的
ステップ 4	Server /chassis* # **commit**	変更をコミットします。
ステップ 5	Server /chassis # **show detail**	（任意）サーバのプロパティを表示します。これで、IOS ロックアウトの現在のステータス（ロックされているか、またはロック解除されているか）を判断できます。

次の例では、Cisco IOS CLI を使用して設定変更が行われないようにしています。

```
Server# scope chassis
Server /chassis # show detail
 Chassis:
  Power: on
  Power Button: unlocked
  IOS Lockout: unlocked
  Serial Number: FHH16150031
  Product Name: E160DP
  PID : UCS-E160DP-M1/K9
  UUID: 0024C4F4-89F2-0000-A7D1-770BCA4B8924
  Description
Server /chassis # set ios-lockout locked
Server /chassis* # commit
Server /chassis # show detail
 Chassis:
  Power: on
  Power Button: unlocked
  IOS Lockout: locked
  Serial Number: FHH16150031
  Product Name: E160DP
  PID : UCS-E160DP-M1/K9
  UUID: 0024C4F4-89F2-0000-A7D1-770BCA4B8924
  Description
```

Cisco IOS CLI 設定変更のロック解除

この手順を使用して、Cisco IOS CLI で設定を変更できるようにします。

はじめる前に

このタスクを実行するには、user または admin 権限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 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 detail**	（任意）サーバのプロパティを表示します。これで、IOS ロックアウトの現在のステータス（ロックされているか、またはロック解除されているか）を判断できます。

	コマンドまたはアクション	目的
ステップ 3	Server /chassis # **set ios-lockout unlocked**	Cisco IOS CLI を使用して設定を変更できるようにします。
ステップ 4	Server /chassis* # **commit**	変更をコミットします。
ステップ 5	Server /chassis # **show detail**	（任意）サーバのプロパティを表示します。これで、IOS ロックアウトの現在のステータス（ロックされているか、またはロック解除されているか）を判断できます。

次の例では、Cisco IOS CLI を使用して設定を変更できるようにしています。

```
Server# scope chassis
Server /chassis # show detail
 Chassis:
  Power: on
  Power Button: unlocked
  IOS Lockout: locked
  Serial Number: FHH16150031
  Product Name: E160DP
  PID : UCS-E160DP-M1/K9
  UUID: 0024C4F4-89F2-0000-A7D1-770BCA4B8924
  Description
Server /chassis # set ios-lockout unlocked
Server /chassis* # commit
Server /chassis # show detail
 Chassis:
  Power: on
  Power Button: unlocked
  IOS Lockout: unlocked
  Serial Number: FHH16150031
  Product Name: E160DP
  PID : UCS-E160DP-M1/K9
  UUID: 0024C4F4-89F2-0000-A7D1-770BCA4B8924
  Description
```

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。

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 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**	確認のプロンプトが表示されたら、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   PID            UUID
----- ------------- -------------  -------------  ------------------------------------
on    FOC16161F1P   E160D          UCS-E160D-M... 1255F7F0-9F17-0000-E312-94B74999D9E7
```

サーバの電源オフ

はじめる前に

このタスクを実行するには、user または admin 権限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 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   PID            UUID
----- ------------- -------------  -------------  ------------------------------------
off    FOC16161F1P   E160D          UCS-E160D-M... 1255F7F0-9F17-0000-E312-94B74999D9E7
```

サーバ電源の再投入

はじめる前に

このタスクを実行するには、user または admin 権限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 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**	確認のプロンプトが表示されたら、サーバの電源を再投入します。 （注） • サーバ電源の再投入は、サーバの実際の電源ボタンを押して電源をオフにした後、電源をオンにする動作と同じです。 • 電源のハードリセットは、サーバの実際のリセット ボタンを押す動作と同じです。

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
This operation will change the server's power state.
Continue?[y|N]y
```

サーバの前面パネルの電源ボタンのロック

この手順を使用して、物理サーバの前面パネルにある物理電源ボタンを無効にします。 電源ボタンを無効にすると、前面パネルの電源ボタンを使用して、サーバの電源をオンまたはオフにすることができなくなります。

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 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 detail**	（任意）サーバのプロパティを表示します。これで、電源ボタンの現在のステータス（ロックされているか、またはロック解除されているか）を判断できます。
ステップ 3	Server /chassis # **set power-button locked**	電源ボタンを無効にします。 前面パネルの電源ボタンを使用して、サーバの電源をオンまたはオフにすることはできません。
ステップ 4	Server /chassis* # **commit**	変更をコミットします。
ステップ 5	Server /chassis # **show detail**	（任意）サーバのプロパティを表示します。これで、電源ボタンの現在のステータス（ロックされているか、またはロック解除されているか）を判断できます。

次の例では、物理サーバの前面パネルにある物理電源ボタンを無効にしています。

```
Server# scope chassis
Server /chassis # show detail
 Chassis:
  Power: on
  Power Button: unlocked
  IOS Lockout: unlocked
  Serial Number: FHH16150031
  Product Name: E160DP
  PID : UCS-E160DP-M1/K9
  UUID: 0024C4F4-89F2-0000-A7D1-770BCA4B8924
  Description
Server /chassis # set power-button locked
Server /chassis* # commit
Server /chassis # show detail
 Chassis:
  Power: on
  Power Button: locked
  IOS Lockout: unlocked
  Serial Number: FHH16150031
  Product Name: E160DP
  PID : UCS-E160DP-M1/K9
  UUID: 0024C4F4-89F2-0000-A7D1-770BCA4B8924
  Description
```

サーバの前面パネルの電源ボタンのロック解除

この手順を使用して、物理サーバの前面パネルにある物理電源ボタンを有効にします。 電源ボタンを有効にすると、前面パネルの電源ボタンを使用して、サーバの電源をオンまたはオフにすることができます。

はじめる前に

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

手順

	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 detail**	（任意）サーバのプロパティを表示します。これで、電源ボタンの現在のステータス（ロックされているか、またはロック解除されているか）を判断できます。
ステップ 3	Server /chassis # **set power-button unlocked**	電源ボタンを有効にします。 前面パネルの電源ボタンを使用して、サーバの電源をオンまたはオフにすることができます。
ステップ 4	Server /chassis* # **commit**	変更をコミットします。
ステップ 5	Server /chassis # **show detail**	（任意）サーバのプロパティを表示します。これで、電源ボタンの現在のステータス（ロックされているか、またはロック解除されているか）を判断できます。

次の例では、物理サーバの前面パネルにある物理電源ボタンを有効にしています。

```
Server# scope chassis
Server /chassis # show detail
 Chassis:
  Power: on
  Power Button: locked
  IOS Lockout: unlocked
  Serial Number: FHH16150031
  Product Name: E160DP
  PID : UCS-E160DP-M1/K9
  UUID: 0024C4F4-89F2-0000-A7D1-770BCA4B8924
  Description
Server /chassis # set power-button unlocked
Server /chassis* # commit
Server /chassis # show detail
 Chassis:
  Power: on
  Power Button: unlocked
  IOS Lockout: unlocked
  Serial Number: FHH16150031
  Product Name: E160DP
  PID : UCS-E160DP-M1/K9
  UUID: 0024C4F4-89F2-0000-A7D1-770BCA4B8924
  Description
```

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

Server /bios #
```

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 # **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。	CLI コマンド、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、次のトピックを参照してください。 • 詳細：プロセッサ BIOS 設定, （33 ページ） • 詳細：メモリ BIOS 設定, （40 ページ） • 詳細：シリアル ポート BIOS 設定, （41 ページ） • 詳細：USB BIOS 設定, （41 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。 変更内容は次のサーバのリブート時に適用されます。サーバの電源が投入されている場合、すぐにリブートするかどうかを質問されます。

次に、Intel Virtualization Technology をイネーブルにする例を示します。

```
Server# scope bios
Server /bios # scope advanced
Server /bios/advanced # set IntelVTD 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 # **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。	CLI コマンド、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、次のトピックを参照してください。 • サーバ管理 BIOS 設定, （41 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。 変更内容は次のサーバのリブート時に適用されます。 サーバの電源が投入されている場合、すぐにリブートするかどうかを質問されます。

次に、ボー レートを 9.6k に設定する例を示します。

```
Server# scope bios
Server /bios # scope server-management
Server /bios/server-management # set BaudRate 9.6k
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 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
```

BIOS パスワードのクリア

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope bios**	BIOS コマンド モードを開始します。
ステップ 2	Server /bios # **clear-bios-password**	BIOS パスワードをクリアします。 パスワードのクリア処理を有効にするには、サーバをリブートする必要があります。 サーバがリブートすると、新しいパスワードを作成するように求められます。

次に、BIOS パスワードをクリアする例を示します。

```
Server# scope bios
Server /bios # clear-bios-password
This operation will clear the BIOS Password.
Note: Server should be rebooted to clear BIOS password.
Continue?[y|N]y
```

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
```

サーバ BIOS 設定

次の各表に、表示および設定が可能なサーバ BIOS 設定を示します。

各設定には、表内の設定名の下に CLI の **set** コマンドが示されています。また、設定の説明内にコマンド オプションが一覧されています。 各設定のデフォルトを表示するには、**set** コマンドに続けて疑問符を入力します。表示されたオプション キーワード内で、デフォルトのオプションにはアスタリスクが付けられています。

（注） お使いのサーバでの BIOS 設定のサポート状況を確認することを推奨します。 搭載されているハードウェアによっては、一部の設定がサポートされていない場合があります。

詳細：プロセッサ BIOS 設定

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**	パッケージ内の論理プロセッサ コアの状態を設定します。この設定をディセーブルにすると、ハイパースレッディングもディセーブルになります。次のいずれかになります。 • [All]：すべての論理プロセッサ コアでマルチ プロセッシングをイネーブルにします。 • [1] ～ [*n*]：サーバ上で動作できる論理プロセッサ コアの数を指定します。マルチプロセッシングをディセーブルにし、サーバ上で動作する論理プロセッサ コアを 1 つだけにするには、[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**	プロセッサ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。 次のいずれかになります。 • [Disabled]：プロセッサから C3 レポートを送信しません。 • [ACPI_C2]：C2 フォーマットを使用してプロセッサから C3 レポートを送信します。 • [ACPI_C3]：C3 フォーマットを使用してプロセッサから C3 レポートを送信します。

名前	説明
[Processor C6 Report] **set ProcessorC6Report**	プロセッサ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。 次のいずれかになります。 • [Disabled]：プロセッサから C6 レポートを送信しません。 • [Enabled]：プロセッサから C6 レポートを送信します。
[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） この値を設定するには、[CPU Performance] 設定で [Custom] を選択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、Intel Adjacent Cache-Line Prefetch メカニズムを使用して必要に応じてデータを取得するかどうか。次のいずれかになります。 • [Disabled]：Adjacent Cache-Line Prefetch メカニズムは使用しません。 • [Enabled]：キャッシュの問題が検出されたときに Adjacent Cache-Line Prefetch メカニズムを使用します。 （注） この値を設定するには、[CPU Performance] 設定で [Custom] を選択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。

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][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。 • [C2_state]：システム レベルの調整が進行中のため、電力消費が多くなります。 調整が完了するまで、パフォーマンス上の問題が発生する可能性があります。 • [C6_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。 このオプションでは、節約される電力が C0 または C2 よりも多くなりますが、サーバがフル パワーに戻るまで、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。
[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。

名前	説明
[Demand Scrub] **set DemandScrub**	メモリ スクラブをオンデマンドで実行できるかどうか。次のいずれかになります。 • [Disabled]：メモリ スクラブをオン デマンドで実行できません。 • [Enabled]：メモリ スクラブをオン デマンドで実行できます。エラーが発生した場合、システムは修正を試みるか、その場所に、読み込めないというマークを付けます。このプロセスにより、システムの実行速度が向上し、データ処理エラーが減少します。
[Device Tagging] **set DeviceTagging**	説明、アドレス、および名前を含むさまざまな情報に基づいて、デバイスとインターフェイスをグループ化できるかどうか。 次のいずれかになります。 • [Disabled]：デバイスとインターフェイスをグループ化できません。 • [Enabled]：デバイスとインターフェイスをグループ化できます。

詳細：メモリ **BIOS** 設定

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]：一定のメモリ冗長性でシステムの信頼性を強化しながら、ミラーリングの場合よりも多くのメモリをオペレーティング システムが使用できるようにします。

詳細：シリアル ポート BIOS 設定

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。

詳細：USB BIOS 設定

名前	説明
[USB Port 0] **set USBPort0**	プロセッサで USB ポート 0 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 USB ポート 0 を使用しません。 • [Enabled]：プロセッサで USB ポート 0 を使用します。
[USB Port 1] **set USBPort1**	プロセッサで USB ポート 1 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 USB ポート 1 を使用しません。 • [Enabled]：プロセッサで USB ポート 1 を使用します。

サーバ管理 BIOS 設定

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。
[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。 このオプションはブレード サーバおよびラックマウント サーバに対して有効です。 （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）は、隠れ端末の問題によって生じる可能性のあるフレーム衝突を減らすのに役立ちます。 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。
[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] **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。 タイマーが切れる前にオペレーティング システムのブートを完了しない場合、CIMC はシステムをリセットし、エラーがログに記録されます。 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。
[OS Boot Watchdog Timer Policy] **set OSBootWatchdogTimerPolicy**	ウォッチドッグ タイマーが切れたとき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。 • [Do Nothing]：OS のブート中にウォッチドッグ タイマーが切れたときに、サーバの電源状態は変化しません。 • [Power Down]：OS のブート中にウォッチドッグ タイマーが切れた場合、サーバの電源はオフになります。 • [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。
set ResumeOnACPowerLoss	

第 4 章

RAID の管理

- RAID オプション，45 ページ
- RAID の設定，49 ページ
- RAID 設定の削除，52 ページ
- 物理ドライブの状態の変更，53 ページ
- 物理ドライブの再構築，54 ページ
- 物理ドライブの内容の削除，55 ページ
- ストレージ コントローラ上での自動再構築のイネーブル化，57 ページ
- 仮想ドライブの削除，58 ページ
- 仮想ドライブの整合性検査の実行，58 ページ
- 仮想ドライブの再構築のオプション，60 ページ
- ディスク ドライブのブート可能化，64 ページ

RAID オプション

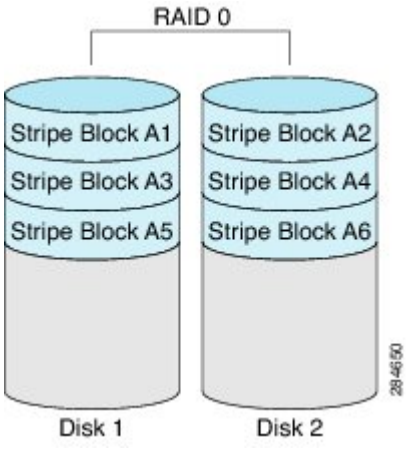
E シリーズ サーバのデータ ファイルは、ローカルの Redundant Array of Inexpensive Disks（RAID）に保存することもできます。 次の RAID レベルがサポートされています。

- シングルワイドの E シリーズ サーバでは、RAID 0 および RAID 1 レベルがサポートされます。
- ダブルワイドの E シリーズ サーバでは、RAID 0、RAID 1、および RAID 5 レベルがサポートされます。
- PCIe オプションを搭載したダブルワイドの E シリーズ サーバでは、RAID 0 および RAID 1 レベルがサポートされます。

RAID 0

RAID 0 では、データは 1 台以上のディスク ドライブにわたるストライプ ブロックに冗長性（ミラーリング）なしで均等に保存されます。 すべてのディスク ドライブのデータは異なります。

図 *1*：*RAID 0*



RAID 1 と比較すると、RAID 0 では両方のディスク ドライブがデータの保存に使用されるため、記憶域が増加します。 2 台のディスク ドライブ内で読み取り操作と書き込み操作が並行して発生するため、パフォーマンスが向上します。

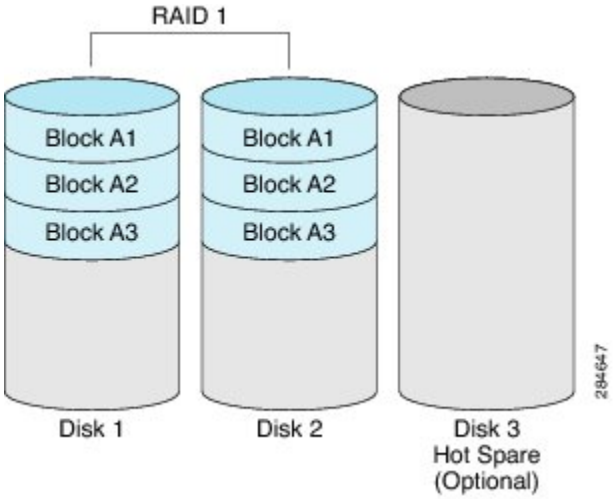
ただし、耐障害性、エラーチェック、ホットスペア、ホットスワップはありません。 一方のディスク ドライブで障害が発生した場合は、アレイ全体のデータが破壊されます。 エラー チェックやホットスワップの機能がないため、アレイは回復不能なエラーの影響を受けやすくなります。

RAID 1

RAID 1 は、ディスク ドライブのミラー セットを作成します。この場合、両方のディスク ドライブ内でデータがまったく同じになるため、冗長性とハイアベイラビリティが実現されます。一方のディスク ドライブで障害が発生した場合は、他方のディスク ドライブが引き継ぎ、データは保持されます。

RAID 1 では、ホット スペア ディスク ドライブを使用することもできます。 ホット スペア ドライブは、常にアクティブであり、フェールオーバー時のホット スタンバイ ドライブとして待機しています。

図 *2*：*RAID 1*



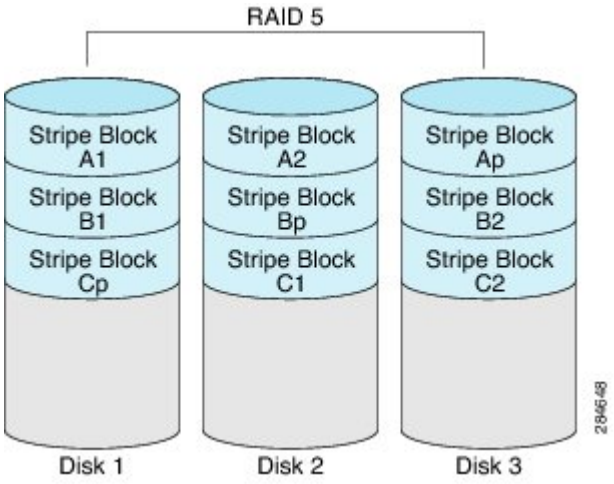
RAID 1 では、耐障害性とホットスワップがサポートされます。 1 台のディスク ドライブで障害が発生した場合は、障害のあるディスク ドライブを取り外して新しいディスク ドライブに交換することができます。

ただし、RAID 0 と比較すると、潜在的な合計ディスク領域の半分しか保存に使用できないため記憶域が減少します。また、パフォーマンスにも影響があります。

RAID 5

RAID 5 では、データがすべてのディスク ドライブにわたって保存され、各ドライブにパリティ データが分散されます。それにより、低コストで冗長性が実現されます。

図 *3* : *RAID 5*



RAID 5 は、RAID 1 よりも大きいデータ ストレージ容量と、RAID 0 よりも優れたデータ保護を提供します。 さらに、ホット スワップもサポートしています。ただし、パフォーマンスは RAID 1 の方が優れています。

Non-RAID

コンピュータのディスク ドライブが RAID として設定されていない場合、コンピュータは非 RAID モードです。 非 RAID モードは、Just a Bunch of Disks または Just a Bunch of Drives（JBOD）とも呼ばれます。 非 RAID モードでは、耐障害性、エラー チェック、ホットスワップ、ホット スペア、冗長性はサポートされません。

RAID オプションの概要

RAID オプション	説明	利点	欠点
RAID 0	冗長性なしでストライプブロックに均等に保存されるデータ	• 優れたストレージ効率 • パフォーマンスの向上	• エラー チェックなし • 耐障害性なし • ホットスワップなし • 冗長性なし • ホット スペアなし

RAID 1	ディスク ドライブのミラーセットとオプションのホット スペア ディスク ドライブ	• ハイ アベイラビリティ • 耐障害性 • ホット スペア • ホットスワップ	• ストレージの減少 • パフォーマンス上の影響
RAID 5	すべてのディスク ドライブにわたってストライプ ブロックに保存されるデータと分散されたパリティ データ	• RAID 1 よりも優れたストレージ効率 • RAID 0 よりも優れた耐障害性 • 低コストの冗長性 • ホットスワップ	• 低いパフォーマンス
非 RAID	RAID が設定されていないディスク ドライブ JBOD とも呼ばれます	• ポータブル	• エラー チェックなし • 耐障害性なし • ホットスワップなし • 冗長性なし • ホット スペアなし

RAID の設定

仮想ドライブの RAID レベル、ストリップ サイズ、ホスト アクセス権限、ドライブ キャッシング、および初期化パラメータを設定するには、次の手順を実行します。

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。

	コマンドまたはアクション	目的
ステップ 2	Server /chassis # **show storageadapter**	インストールされているストレージカードに関する情報を表示します。 この情報を使用して、ストレージ カードが装着されているスロットを判別できます。
ステップ 3	Server /chassis # **scope storageadapter SLOT-5**	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 physical-drive**	物理ディスク ドライブを表示します。この情報を使用して、物理ドライブのステータスを確認することができます。 （注） RAID を設定するには、物理ドライブのステータスが unconfigured good である必要があります。 物理ドライブのステータスを変更するには、「物理ドライブの状態の変更」を参照してください。
ステップ 5	Server /chassis/storageadapter # **create-virtualdrive** {**-r0** | **-r1** | **-r5**} *physical-drive-numbers* [**QuickInit** | **FullInit** | **NoInit**] [**RW** | **RO** | **Blocked**] [**DiskCacheUnchanged** | **DiskCacheEnable** | **DiskCacheDisable**] [**-strpsz64** | **-strpsz32** | **-strpsz16** | **-strpsz8**]	物理ドライブに指定されている RAID レベルで仮想ドライブを作成します。 次のオプションを指定することもできます。 （注） オプションでは、大文字と小文字は区別されません。 • （任意）初期化のオプション ◦ QuickInit：コントローラがドライブを即時に初期化します。 数秒以内に、仮想ドライブへのデータ書き込みを開始できます。 これがデフォルトのオプションです。 ◦ FullInit：コントローラは新しいコンフィギュレーションの完全な初期化を行います。 初期化が完了するまで、仮想ドライブにデータを書き込むことはできません。 ドライブのサイズが大きい場合、この処理に長時間かかることがあります。 ◦ NoInit：コントローラはドライブの初期化を行いません。 • （任意）アクセス ポリシーのオプション ◦ RW：ホストにドライブへのフルアクセス権があります。 これがデフォルトのオプションです。 ◦ RO：ホストはドライブからのデータ読み取りのみを行えます。 ◦ [Blocked]：ホストはドライブにアクセスできません。

	コマンドまたはアクション	目的
		• （任意）ドライブのキャッシュ オプション ◦ DriveCacheDisable：物理ドライブでキャッシュがディセーブルになります。 （注） これがデフォルトであり、推奨オプションです。 ◦ DriveCacheUnchanged：コントローラは物理ドライブに指定されたキャッシュ ポリシーを使用します。これがデフォルトのオプションです。 ◦ DriveCacheEnable：物理ドライブでキャッシュがイネーブルになります。 • （任意）ストリップ サイズのオプション ◦ -strpsz64：これがデフォルトのオプションです。 ◦ -strpsz32 ◦ -strpsz16 ◦ -strpsz8 **注意** ストリップ サイズを小さく設定した場合の VMware vSphere Hypervisor™ インストールに関する既知の問題があるため、vSphere プラットフォームをインストールするときは、strpsz64 オプションを使用することをお勧めします。
ステップ 6	Server /chassis/storageadapter # **show virtual-drive**	（任意）ストレージカード用の仮想ドライブの情報を表示します。 この情報を使用して、RAID 設定を確認することができます。

次に、RAID を設定する例を示します。

```
Server# scope chassis
Server /chassis # show storageadapter

PCI Slot Product      Name    Serial Number  Firmware Package Build   Product ID Cache
Memory Size
-------- ------------------------------ -------------- ------------------------ --------------
 ---
SLOT-5   LSI MegaRAID SAS     2004 ROMB      20.10.1-0092             LSI Logic   0 MB

Server /chassis # scope storageadapter SLOT-5

Server /chassis /storageadapter# show physical-drive

Slot Number  Controller Status              Manufacturer   Model        Drive  Firmware
Coerced Size   Type
```

```
---------- ---------- ---------------------------------- -------------- --------------
-------------- ---
1            SLOT-5     unconfigured good    TOSHIBA        MBF2600RC    5704   571250 MB
         HDD
2            SLOT-5     unconfigured good    ATA            ST9500620NS  SN01   475883 MB
         HDD

Server /chassis /storageadapter # create-virtualdrive -r0 1 FullInit RW DiskCacheEnable
-strpsz32
---
status: ok
----------------------
Server /chassis /storageadapter # show virtual-drive
Virtual Drive  Status               Name                     Size       RAID Level
-------------- -------------------- ------------------------ ---------- ----------
0              Optimal                                       571250 MB  RAID 0
```

次の作業

ディスク ドライブをブート可能にします。 「ディスク ドライブのブート可能化」を参照してください。

RAID 設定の削除

すべての RAID 設定をクリアするには、この手順を実行します。

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 # **show storageadapter**	インストールされているストレージ カードに関する情報を表示します。この情報を使用して、ストレージ カードが装着されているスロットを判別できます。
ステップ 3	Server /chassis # **scope storageadapter SLOT-5**	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 # **clear-all-raid-config**	すべての RAID 設定をクリアします。 確認プロンプトで [Yes] を選択します。 （注） RAID 設定が削除されると、ディスク ドライブに存在するすべてのデータが失われます。

次に、RAID 設定を削除する例を示します。

```
Server# scope chassis
Server /chassis # show storageadapter

PCI Slot Product      Name    Serial Number  Firmware Package Build   Product ID Cache
```

```
Memory Size
-------- ------------------------------ -------------- ----------------------- --------------
 ---
SLOT-5   LSI MegaRAID SAS     2004 ROMB      20.10.1-0092              LSI Logic   0 MB

Server /chassis # scope storageadapter SLOT-5
Server /chassis /storageadapter # clear-all-raid-config
This operation will clear all RAID configuration.
Warning: All data in the disks would be lost!!!
Are you sure you want to proceed? [Yes|No] Yes
Are you really sure you want to clear all RAID configuration and lose all data? [Yes|No]
Yes
```

物理ドライブの状態の変更

物理ドライブの状態を変更するには、次の手順を実行します。 [hotspare]、[jbod]、または [unconfigured good] を選択できます。

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 # **show storageadapter**	インストールされているストレージ カードに関する情報を表示します。 この情報を使用して、ストレージ カードが装着されているスロットを判別できます。
ステップ 3	Server /chassis # **scope storageadapter SLOT-5**	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 physical-drive**	物理ディスク ドライブを表示します。
ステップ 5	Server /chassis/storageadapter # **scope physical-drive** *slot-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。
ステップ 6	Server /chassis/storageadapter /physical-drive # **show detail**	指定された物理ドライブに関する情報を表示します。
ステップ 7	Server /chassis/storageadapter /physical-drive # **set state {unconfiguredgood | jbod | hotspare}**	物理ドライブの状態を変更します。 [hotspare]、[jbod]、または [unconfigured good] を選択できます。
ステップ 8	Server /chassis/storageadapter /physical-drive* # **commit**	変更をコミットします。
ステップ 9	Server /chassis/storageadapter /physical-drive # **show detail**	指定された物理ドライブに関する情報を表示します。

次に、物理ドライブの状態を変更する例を示します。

```
Server# scope chassis
Server /chassis # show storageadapter

PCI Slot Product      Name    Serial Number  Firmware Package Build   Product ID Cache
Memory Size
-------- ---------------------------- ------------- ---------------------- --------------
 ---
SLOT-5   LSI MegaRAID SAS     2004 ROMB      20.10.1-0092             LSI Logic   0 MB

Server /chassis# scope storageadapter SLOT-5
Server /chassis /storageadapter# show physical-drive

Slot Number  Controller Status               Manufacturer   Model        Drive  Firmware
Coerced Size   Type
-----------  ---------- ------------------------------------ -------------- --------------
-------------- -----
1            SLOT-5     system               TOSHIBA        MBF2600RC    5704   571250 MB
         HDD
2            SLOT-5     unconfigured good    ATA            ST9500620NS  SN01   475883 MB
         HDD

Server /chassis /storageadapter# scope physical-drive 1
Server /chassis /storageadapter/physical-drive# show detail

Slot Number 1:
    Controller: SLOT-5
    Status: system
    Manufacturer: TOSHIBA
    Model: MBF2600RC
    Drive Firmware: 5704
    Coerced Size: 571250 MB
    Type: HDD

Server /chassis /storageadapter/physical-drive# set state hotspare
Server /chassis /storageadapter/physical-drive*# commit
Server /chassis /storageadapter/physical-drive# show detail

Slot Number 1:
    Controller: SLOT-5
    Status: hotspare
    Manufacturer: TOSHIBA
    Model: MBF2600RC
    Drive Firmware: 5704
    Coerced Size: 571250 MB
    Type: HDD
```

物理ドライブの再構築

物理ドライブ上で再構築プロセスを手動で開始するには、次の手順を実行します。

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 # **show storageadapter**	インストールされているストレージ カードに関する情報を表示します。 この情報を使用して、ストレージ カードが装着されているスロットを判別できます。

	コマンドまたはアクション	目的
ステップ 3	Server /chassis # **scope storageadapter SLOT-5**	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 physical-drive**	物理ディスク ドライブを表示します。
ステップ 5	Server /chassis/storageadapter # **scope physical-drive** *slot-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。
ステップ 6	Server /chassis/storageadapter /physical-drive # **rebuild**	物理ドライブを再構築します。
ステップ 7	Server /chassis/storageadapter /physical-drive # **rebuild abort**	（任意）再構築プロセスを停止します。

次に、物理ドライブの状態を変更する例を示します。

```
Server# scope chassis
Server /chassis # show storageadapter

PCI Slot Product      Name    Serial Number  Firmware Package Build   Product ID Cache
Memory Size
-------- ---------------------------- -------------- ----------------------- --------------
 ---
SLOT-5   LSI MegaRAID SAS     2004 ROMB      20.10.1-0092             LSI Logic   0 MB

Server /chassis# scope storageadapter SLOT-5
Server /chassis /storageadapter# show physical-drive

Slot Number  Controller Status               Manufacturer   Model        Drive  Firmware
Coerced Size   Type
------------ ---------- ------------------------------------ -------------- --------------
-------------- -----
1            SLOT-5     system               TOSHIBA        MBF2600RC    5704   571250 MB
         HDD
2            SLOT-5     unconfigured good    ATA            ST9500620NS  SN01   475883 MB
         HDD

Server /chassis /storageadapter# scope physical-drive 1
Server /chassis /storageadapter/physical-drive# rebuild
Server /chassis /storageadapter/physical-drive# rebuild abort
```

物理ドライブの内容の削除

次の手順を使用して、物理ドライブの内容をすべて削除し、ゼロに設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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 storageadapter**	インストールされているストレージ カードに関する情報を表示します。 この情報を使用して、ストレージ カードが装着されているスロットを判別できます。
ステップ 3	Server /chassis # **scope storageadapter SLOT-5**	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 physical-drive**	物理ディスク ドライブを表示します。
ステップ 5	Server /chassis/storageadapter # **scope physical-drive** *slot-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。
ステップ 6	Server /chassis/storageadapter /physical-drive # **erase**	物理ドライブの内容をすべて削除して、ゼロに設定します。 （注） 削除プロセスには、数時間かかることがあります。
ステップ 7	Server /chassis/storageadapter /physical-drive # **erase abort**	（任意）削除プロセスを停止します。

次の例は、物理ドライブの内容の削除方法を示します。

```
Server# scope chassis
Server /chassis # show storageadapter

PCI Slot Product      Name    Serial Number  Firmware Package Build   Product ID Cache
Memory Size
-------- ------------------------------ -------------- ------------------------ --------------
 ---
SLOT-5   LSI MegaRAID SAS     2004 ROMB      20.10.1-0092             LSI Logic   0 MB

Server /chassis# scope storageadapter SLOT-5
Server /chassis /storageadapter# show physical-drive

Slot Number  Controller Status               Manufacturer   Model        Drive  Firmware
Coerced Size   Type
------------ ---------- ------------------------------------ -------------- --------------
-------------- -----
1            SLOT-5     system               TOSHIBA        MBF2600RC    5704   571250 MB
         HDD
2            SLOT-5     unconfigured good    ATA            ST9500620NS  SN01   475883 MB
         HDD

Server /chassis /storageadapter# scope physical-drive 1
Server /chassis /storageadapter/physical-drive# erase
Server /chassis /storageadapter/physical-drive# erase abort
```

ストレージコントローラ上での自動再構築のイネーブル化

ディスク ドライブを自動的に再構築するには、次の手順を実行します。 RAID 構成のディスク ドライブの 1 つが劣化状態になったとき、新しいドライブが接続されると、新しいドライブに対して再構築プロセスが自動的に開始されます。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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**	インストールされているストレージ カードに関する情報を表示します。 この情報を使用して、ストレージ カードが装着されているスロットを判別できます。
ステップ 3	Server /chassis # **scope storageadapter SLOT-5**	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 # **set global-hotspare-for-newdrives true**	ストレージ コントローラで自動再構築をイネーブルにします。
ステップ 5	Server /chassis/storageadapter* # **commit**	変更をコミットします。

次に、ストレージ コントローラで自動再作成をイネーブルにする例を示します。

```
Server# scope chassis
Server /chassis # show storageadapter
PCI Slot Product      Name    Serial Number  Firmware Package Build   Product ID Cache
Memory Size
-------- ------------------------------ -------------- ------------------------ --------------
 ---
SLOT-5   LSI MegaRAID SAS     2004 ROMB      20.10.1-0092             LSI Logic   0 MB

Server /chassis# scope storageadapter SLOT-5
Server /chassis /storageadapter# set global-hotspare-for-newdrives true
Server /chassis /storageadapter*# commit
```

仮想ドライブの削除

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 # **show storageadapter**	インストールされているストレージ カードに関する情報を表示します。この情報を使用して、ストレージ カードが装着されているスロットを判別できます。
ステップ 3	Server /chassis # **scope storageadapter SLOT-5**	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 virtual-drive**	仮想ドライブ番号を含む仮想ドライブ情報を表示します。この番号は、仮想ドライブを削除するために必要です。
ステップ 5	Server /chassis/storageadapter # **delete virtual-drive** *drive-number*	指定した仮想ドライブを削除します。
ステップ 6	Server /chassis/storageadapter* # **commit**	変更をコミットします。

次の例は、仮想ドライブの削除方法を示します。

```
Server# scope chassis
Server /chassis # show storageadapter
PCI Slot Product      Name    Serial Number  Firmware Package Build   Product ID Cache
Memory Size
-------- ------------------------------ -------------- ------------------------ --------------
 ---
SLOT-5   LSI MegaRAID SAS     2004 ROMB      20.10.1-0092             LSI Logic   0 MB

Server /chassis# scope storageadapter SLOT-5
Server /chassis /storageadapter # show virtual-drive
Virtual Drive  Status              Name                     Size       RAID Level
-------------- ------------------- ------------------------ ---------- ----------
0              Optimal                                      571250 MB  RAID 0

Server /chassis /storageadapter # delete virtual-drive 0
Server /chassis /storageadapter *# commit
```

仮想ドライブの整合性検査の実行

ドライブの整合性を確認するには、次の手順を使用します。

- RAID 5：この手順で、パリティ ストライプ ブロックすべてのデータが正しいかどうかを確認します。

- RAID 1：この手順で、両方のディスク ドライブのデータが同じであるかどうかを確認します。

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 # **show storageadapter**	インストールされているストレージ カードに関する情報を表示します。 この情報を使用して、ストレージカードが装着されているスロットを判別できます。
ステップ 3	Server /chassis # **scope storageadapter SLOT-5**	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 # **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 5	Server /chassis/storageadapter /virtual-drive # **verify**	ドライブの整合性を確認します。 • RAID 5：パリティ ストライプ ブロックすべてのデータが正しいかどうかを確認します。 • RAID 1：両方のディスク ドライブのデータが同じであるかどうかを確認します。
ステップ 6	Server /chassis/storageadapter /virtual-drive # **verify abort**	（任意）確認プロセスを停止します。
ステップ 7	Server /chassis/storageadapter /virtual-drive # **show detail**	指定された仮想ドライブに関する情報を表示します。

次に、仮想ドライブの整合性検査を実行する例を示します。

```
Server# scope chassis
Server /chassis # show storageadapter

PCI Slot Product      Name    Serial Number  Firmware Package Build   Product ID Cache
Memory Size
-------- ------------------------------ ------------- ----------------------- --------------
 ---
SLOT-5   LSI MegaRAID SAS     2004 ROMB      20.10.1-0092             LSI Logic   0 MB

Server /chassis# scope storageadapter SLOT-5
Server /chassis /storageadapter# scope virtual-drive 0
Server /chassis /storageadapter/virtual-drive# verify
---
status: ok
...
Server /chassis /storageadapter/virtual-drive# show detail
Status: Optimal
```

```
Name:
Size: 475883 MB
RAID Level: RAID 1
Target ID: 0
Stripe Size: 64 KB
Drives Per Span: 2
Span Depth: 1
Access Policy: Read-Write
Disk Cache Policy: Unchanged
Write Cache Policy: Write Through
Cache Policy: Direct
Read Ahead Policy: None
Auto Snapshot: false
Auto Delete Oldest: true
Allow Background Init: true
Consistency Check Progress: 0 %
Consistency Check Elapsed Seconds: 0 s
```

仮想ドライブの再構築のオプション

新しい RAID レベルに仮想ドライブを移行（再構築）するには、物理ドライブの追加または削除が必要な場合があります。 物理ドライブを追加または削除するときに、仮想ドライブのサイズは維持または増加されます。

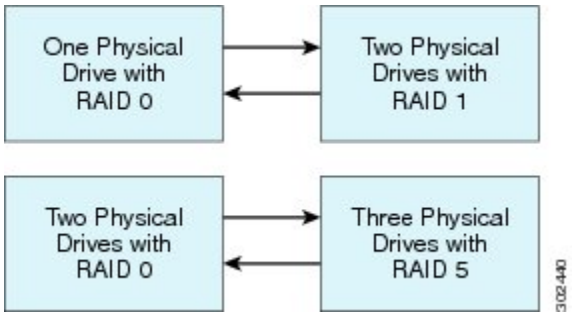
仮想ドライブのサイズを維持したり、増やしたりすることはできますが、減らすことはできません。 たとえば、RAID 0 で 2 台の物理ドライブがある場合、同じ台数のドライブで RAID 1 に移行することはできません。 RAID 1 では、ミラーリングされた一連のディスク ドライブが作成され、これによって、仮想ドライブのサイズが元のサイズの半分にまで減少します。これは、サポートされていません。

（注） 仮想ドライブの再構築プロセスは、完了までに数時間かかることがあります。 再構築プロセス中も、システムを引き続き使用できます。

仮想ドライブのサイズを維持するためのオプション

仮想ドライブを新しい RAID レベルに移行した際に仮想ドライブのサイズが維持されるオプションについては、次の図とその後に続く表を参照してください。

図 *4*：仮想ドライブ サイズが維持されるオプション



次の表に、仮想ドライブのサイズが維持されるオプションの一覧と、仮想ドライブを特定の RAID レベルに移行する際に追加または削除しなければならない物理ドライブの台数に関する情報を示します。

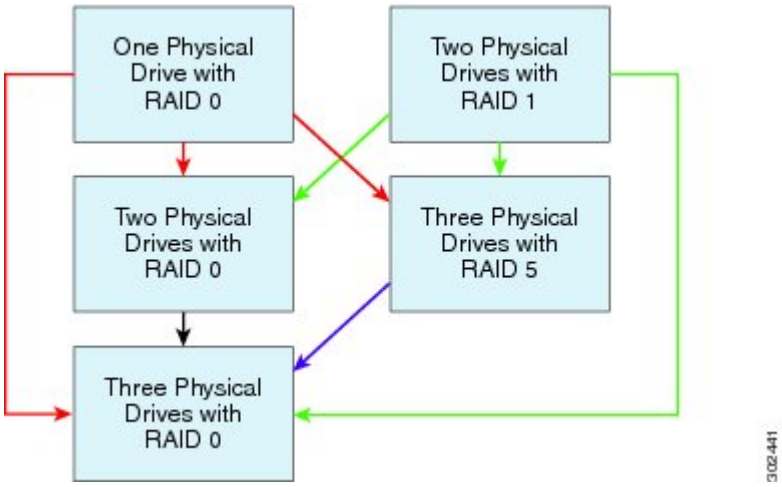
表 *2*：仮想ドライブ サイズの維持

変更前：	移行後：	ディスクの追加または削除
RAID 0 で物理ドライブが 1 台	RAID 1 で物理ドライブが 2 台	ディスクを 1 台追加します。
RAID 1 で物理ドライブが 2 台	RAID 0 で物理ドライブが 1 台	ディスクを 1 台削除します。
RAID 0 で物理ドライブが 2 台	RAID 5 で物理ドライブが 3 台	ディスクを 1 台追加します。
RAID 5 で物理ドライブが 3 台	RAID 0 で物理ドライブが 2 台	ディスクを 1 台削除します。

仮想ドライブのサイズを増やすためのオプション

仮想ドライブを新しい RAID レベルに移行したときに仮想ドライブのサイズが増加するオプションについては、次の図とその後に続く表を参照してください。

図 *5*：仮想ドライブ サイズが増加するオプション



次の表に、仮想ドライブのサイズが増加するオプションの一覧と、仮想ドライブを特定の RAID レベルに移行する際に追加または削除しなければならない物理ドライブの台数に関する情報を示します。

表 *3*：仮想ドライブ サイズの増加

変更前：	移行後：	ディスクの追加または削除
RAID 0 で物理ドライブが 1 台 図の赤い矢印を参照してください。	RAID 0 で物理ドライブが 2 台	ディスクを 1 台追加します。
	RAID 5 で物理ドライブが 3 台	ディスクを 2 台追加します。
	RAID 0 で物理ドライブが 3 台	ディスクを 2 台追加します。
RAID 1 で物理ドライブが 2 台 図の緑の矢印を参照してください。	RAID 0 で物理ドライブが 2 台	—
	RAID 5 で物理ドライブが 3 台	ディスクを 1 台追加します。
	RAID 0 で物理ドライブが 3 台	ディスクを 1 台追加します。

変更前：	移行後：	ディスクの追加または削除
RAID 0 で物理ドライブが 2 台 図の黒い矢印を参照してください。	RAID 0 で物理ドライブが 3 台	ディスクを 1 台追加します。
RAID 5 で物理ドライブが 3 台 図の紫の矢印を参照してください。	RAID 0 で物理ドライブが 3 台	—

仮想ドライブの再構築

指定された RAID レベルに仮想ドライブを移行するために、物理ドライブを追加または削除するには、この手順を使用します。

はじめる前に

仮想ドライブの再構築のオプション，（60 ページ）を参照してください。

手順

	コマンドまたはアクション	目的
ステップ 1	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**	インストールされているストレージ カードに関する情報を表示します。 この情報を使用して、ストレージカードが装着されているスロットを判別できます。
ステップ 3	Server /chassis # **scope storageadapter SLOT-5**	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 # **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 5	Server /chassis/storageadapter /virtual-drive # **reconstruct** {**-r0** | **-r1** | **-r5**} [**-add** | **-rmv**] *new-physical-drive-slot-number(s)*	新しい指定RAID レベルに仮想ドライブを移行するために物理ドライブを追加または削除します。 • -r0 | -r1 | -r5：使用可能な RAID レベルは RAID 0、RAID 1、または RAID 5 です。 • - add | - rmv：物理ドライブを追加または削除します。

	コマンドまたはアクション	目的
ステップ 6	Server /chassis/storageadapter /virtual-drive # **show detail**	指定された仮想ドライブに関する情報を表示します。

次に、最初に RAID 1 として設定されていた 2 台のディスクのうち 1 台を RAID 0 に移行する例を示します。

```
Server# scope chassis
Server /chassis # show storageadapter

PCI Slot Product      Name    Serial Number  Firmware Package Build   Product ID Cache
Memory Size
-------- ------------------------------ -------------- ----------------------- --------------
 ---
SLOT-5   LSI MegaRAID SAS     2004 ROMB      20.10.1-0092             LSI Logic   0 MB

Server /chassis# scope storageadapter SLOT-5
Server /chassis /storageadapter# scope virtual-drive 0
Server /chassis /storageadapter/virtual-drive# reconstruct -r0 -rmv 1
---
status: ok
...
Server /chassis /storageadapter/virtual-drive# show detail
Status: Optimal
    Status: Optimal
    Name:
    Size: 475883 MB
    RAID Level: RAID 1
    Target ID: 0
    Stripe Size: 64 KB
    Drives Per Span: 2
    Span Depth: 1
    Access Policy: Read-Write
    Disk Cache Policy: Unchanged
    Write Cache Policy: Write Through
    Cache Policy: Direct
    Read Ahead Policy: None
    Auto Snapshot: false
    Auto Delete Oldest: true
    Allow Background Init: true
    ReConstruct Progress: 0 %
    ReConstruct Elapsed Seconds: 3 s
```

ディスク ドライブのブート可能化

RAID の設定後、ディスク ドライブをブート可能にする必要があります。 ディスク ドライブをブート可能にするには、次の手順を実行します。

はじめる前に

ディスク ドライブに RAID を設定します。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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**	インストールされているストレージ カードに関する情報を表示します。 この情報を使用して、ストレージ カードが装着されているスロットを判別できます。
ステップ 3	Server /chassis # **scope storageadapter SLOT-5**	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 physical-drive**	物理ディスク ドライブを表示します。 （注） 物理ドライブのステータスは次のいずれかになります。 • system：JBOD モード。 ドライブが RAID として設定されていません。 • online：RAID モード。 • [unconfigured good]：ドライブをドライブ グループまたはホット スペア プールに割り当てることができます。 ドライブにモードは設定されていません。 • [hotspare]：ドライブをスペア ドライブに指定します。 ドライブにモードは設定されていません。
ステップ 5	Server /chassis/storageadapter # **set boot-drive {pd1 | pd2 | pd3 | vd0}**	ディスク ドライブをブート可能にします。 （注） ディスク ドライブをブート可能にするには、ドライブのステータスが system である必要があります。 ステータスが system である場合、ドライブは JBOD（RAID ではない）モードです。
ステップ 6	Server /chassis/storageadapter # **commit**	変更をコミットします。
ステップ 7	Server /chassis/storageadapter # **show settings**	設定を表示します。

次に、CIMC CLI を使用してディスク ドライブをブート可能にする例を示します。

```
Server# scope chassis
Server /chassis# show storageadapter
```

```
PCI Slot Product      Name    Serial Number  Firmware Package Build   Product ID Cache
Memory Size
-------- ------------------------------ -------------- ----------------------- --------------
 ---
SLOT-5   LSI MegaRAID SAS     2004 ROMB      20.10.1-0092             LSI Logic   0 MB

Server /chassis# scope storageadapter SLOT-5
Server /chassis /storageadapter# show physical-drive

Slot Number  Controller Status               Manufacturer   Model        Drive  Firmware
Coerced Size   Type
-----------  ---------- ------------------------------------ -------------- --------------
-------------- -----
1            SLOT-5     system               TOSHIBA        MBF2600RC    5704   571250 MB
         HDD
2            SLOT-5     unconfigured good    ATA            ST9500620NS  SN01   475883 MB
         HDD

   Server /chassis /storageadapter# set boot-drive pd1
Server /chassis /storageadapter*# commit
Server /chassis /storageadapter# show settings
Boot Drive: pd1
```

第 5 章

サーバのプロパティの表示

この章は、次の内容で構成されています。

- サーバのプロパティの表示，67 ページ
- 実際のブート順の表示，68 ページ
- CIMC 情報の表示，69 ページ
- CPU のプロパティの表示，69 ページ
- メモリのプロパティの表示，70 ページ
- 電源のプロパティの表示，71 ページ
- ストレージのプロパティの表示，71 ページ
- PCI アダプタのプロパティの表示，75 ページ
- 電源ポリシーの統計情報の表示，76 ページ
- ハード ドライブのプレゼンスの表示，76 ページ
- インターフェイスの MAC アドレスの表示，77 ページ
- CIMC ネットワーク接続ステータスの表示，78 ページ

サーバ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 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# scope chassis
Server /chassis # show detail
Chassis:
    Power: on
    Power Button: unlocked
    IOS Lockout: unlocked
    Serial Number: FOC16161F1P
    Product Name: E160D
    PID : UCS-E160D-M1/K9
    UUID: 1255F7F0-9F17-0000-E312-94B74999D9E7
    Description
```

実際のブート順の表示

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 actual-boot-order**	BIOS ステータスの詳細を表示します。

次の例では、実際のブート順を表示しています。

```
Server# scope bios
Server /bios # show actual-boot-order
Boot Order   Type                      Boot Device
------------ ------------------------- ----------------------------------
1            Internal EFI Shell        Internal EFI Shell
2            CD/DVD                    Linux Virtual CD/DVD 0324
3            HDD                       PCI RAID Adapter
4            HDD                       Cypress
5            HDD                       Linux Virtual FDD/HDD 0324
6            FDD                       Linux Virtual Floppy 0324
7            Network Device (PXE)      BRCM MBA Slot 0301 v15.2.7
8            Network Device (PXE)      BRCM MBA Slot 0302 v15.2.7
9            Network Device (PXE)      BRCM MBA Slot 0300 v15.2.7
```

CIMC 情報の表示

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。

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 # **show** [**detail**]	CIMC ファームウェア、現在時刻、およびブートローダ バージョンを表示します。

次に、CIMC に関する情報の例を示します。

```
Server# scope cimc
Server /cimc # show detail
CIMC:
    Firmware Version: 1.0(1.20120417172632)
    Current Time: Thu Apr 26 12:11:44 2012
    Boot-loader Version: 1.0(1.20120417172632).16
```

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     E5-2418L 0 @ 2.00GHz
```

```
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
-------------------- --------------- ------------------- ---------------

Node0_Dimm0          8192 MB         1333                DDR3
Node0_Dimm1          8192 MB         1333                DDR3
Node0_Dimm2          8192 MB         1333                DDR3
```

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 Node0_Dimm0:
 Capacity: 8192 MB
 Channel Speed (MHz): 1333
 Channel Type: DDR3
 Memory Type Detail: Registered (Buffered)
 Bank Locator: Node0_Bank0
 Visibility: Yes
 Operability: Operable
 Manufacturer: Samsung
 Part Number: M393B1K70DH0-
 Serial Number: 86A7D514
 Asset Tag: Dimm0_AssetTag
 Data Width: 64 bits
 Name Node0_Dimm1:
 Capacity: 8192 MB
```

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: 1334 MHz
 Total Memory: 24576 MB
 Effective Memory: 24576 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: Reserved
Memory Configuration: Maximum Performance
```

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 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 # **show** [**detail**]	サーバ電力使用量の情報を表示します。

この例では、シングルワイドの E シリーズ サーバの詳細な電源プロパティを表示します。

```
 Server# scope power-cap
 Server /power-cap # show detail
  Cur Consumption (W): 36.10 W
  Max Consumption (W): 075
  Min Consumption (W): 36.10 W
Server /power-cap #
```

この例では、ダブルワイドの E シリーズ サーバの詳細な電源プロパティを表示します。

```
 Server# scope power-cap
 Server /power-cap # show detail
  Cur Consumption (W): 43.1 W
  Max Consumption (W): 160
  Min Consumption (W): 43.1 W
Server /power-cap #
```

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すべての MegaRAID 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は、CIMC 経由で管理できません。
ステップ 3	Server /chassis # **scope storageadapter SLOT-5**	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 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 5	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 6	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 7	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 8	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 9	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 10	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。

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

Controller Product Name                Firmware Package Build Product ID     Cache Memory
Size
---------- --------------------------- ---------------------- -------------- -----------------

SLOT-5     LSI MegaRAID SAS 2004 ROMB  20.10.1-0092           LSI Logic      0 MB
```

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-5**	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** [*slot-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** *slot-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。
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 security** [**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。

次に、SLOT-5 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する例を示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-5
Server /chassis/storageadapter # scope physical-drive 1
Server /chassis/storageadapter/physical-drive # show general
Slot Number 1:
    Controller: SLOT-5
    Enclosure Device ID: 64
    Device ID: 3
    Sequence Number: 2
    Media Error Count: 0
    Other Error Count: 12
    Predictive Failure Count: 0
    Link Speed: 6.0 Gb/s
    Interface Type: SATA
    Media Type: HDD
    Block Size: 512
```

```
    Block Count: 1953525168
    Raw Size: 953869 MB
    Non Coerced Size: 953357 MB
    Coerced Size: 952720 MB
    SAS Address 0: 4433221100000000
    SAS Address 1:
    Connected Port 0:
    Connected Port 1:
    Connected Port 2:
    Connected Port 3:
    Connected Port 4:
```

次に、SLOT-5 という名前のストレージ カードの物理ドライブ番号 1 に関するステータス情報を表示する例を示します。

```
Server# scope chassis
Server /chassis # scope storageadapter SLOT-5
Server /chassis/storageadapter # scope physical-drive 1
Server /chassis/storageadapter/physical-drive # show status
Slot Number 1:
   Controller: SLOT-5
   State: system
   Online: true
   Fault: false
```

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-5**	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。

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 # scope storageadapter SLOT-5
Server /chassis/storageadapter # show virtual-drive
Virtual Drive  Status              Name                     Size       RAID Level
-------------- ------------------- ------------------------ ---------- ----------
```

```
0             Optimal                                          571250 MB  RAID 1

Server /chassis/storageadapter # show virtual-drive-count
PCI Slot SLOT-5:
    Virtual Drive Count: 1
    Degraded Virtual Drive Count: 0
    Offline Virtual Drive Count: 0
Server /chassis/storageadapter # scope virtual-drive 0
Server /chassis/storageadapter/virtual-drive # show physical-drive
Span  Physical Drive Status     Starting Block Number Of Blocks
----- -------------- ---------- -------------- ----------------
0     2              online     0              1169920000
0     1              online     0              1169920000
```

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 #
```

電源ポリシーの統計情報の表示

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。

この例では、シングルワイドの E シリーズ サーバの詳細な電力統計情報を表示します。

```
 Server# scope power-cap
 Server /power-cap # show detail
  Cur Consumption (W): 36.10 W
  Max Consumption (W): 075
  Min Consumption (W): 36.10 W
Server /power-cap #
```

この例では、ダブルワイドの E シリーズ サーバの詳細な電力統計情報を表示します。

```
 Server# scope power-cap
 Server /power-cap # show detail
  Cur Consumption (W): 43.1 W
  Max Consumption (W): 160
  Min Consumption (W): 43.1 W
Server /power-cap #
```

ハード ドライブのプレゼンスの表示

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 hdd**	ハード ドライブを表示します。

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 hdd
    Name              Status
--------------------- --------------------
HDD1_PRS              inserted
HDD2_PRS              inserted
HDD3_PRS              inserted
```

インターフェイスの MAC アドレスの表示

システムで定義されたインターフェイスの名前と、各ホスト インターフェイスに割り当てられた 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**]	システムで定義されたインターフェイスの名前と、各ホストインターフェイスに割り当てられた MAC アドレスを表示します。

次の例は、システムで定義されたインターフェイスの名前と、各ホスト インターフェイスに割り当てられた MAC アドレスを表示する方法を示しています。

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # show lom-mac-list
Interface                    MAC Address
---------------------------- --------------------
Console                      00:24:c4:f4:89:ee
GE1                          00:24:c4:f4:89:ef
GE2                          00:24:c4:f4:89:f0
GE3                          00:24:c4:f4:89:f1
```

CIMC ネットワーク接続ステータスの表示

はじめる前に

CIMC ネットワーク接続のステータスを表示するには、接続が検出されている（物理ケーブルがネットワーク インターフェイスに接続されている）かどうかにかかわらず、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 # **show link state [detail]**	接続が検出されている（物理ケーブルがネットワーク インターフェイスに接続されている）かどうかにかかわらず、CIMC ネットワーク接続のステータスが表示されます。

次の例では、CIMC ネットワーク接続のステータスを表示しています。

```
Server# scope cimc
Server /cimc # scope network
Server /cimc/network # show link state
Interface                     State
----------------------------- --------------------
Console                       Link Detected
GE1                           No Link Detected
GE2                           No Link Detected
GE3                           No Link Detected
Dedicated                     Link Detected

Server /cimc/network # show link-state detail
Link State:
    Interface: Console
    State: Link Detected
Link State:
    Interface: GE1
    State: No Link Detected
Link State:
    Interface: GE2
    State: No Link Detected
Link State:
    Interface: GE3
    State: No Link Detected
Link State:
    Interface: Dedicated
    State: Link Detected
```

第 6 章

サーバのセンサーの表示

この章は、次の内容で構成されています。

- 障害サマリーの表示，79 ページ
- 温度センサーの表示，80 ページ
- 電圧センサーの表示，80 ページ
- LED センサーの表示，81 ページ
- ストレージ センサーの表示，82 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。
ステップ 4	Server /fault # **show pef [detail]**	プラットフォームイベントフィルタの概要を表示します。

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 #
```

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 #
```

LED センサーの表示

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、情報が表示されません。

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 led** [**detail**]	外部 LED の名前、状態、および色を表示します。

次の例では、外部 LED に関する情報を表示しています。

```
Server# scope chassis
Server /chassis # show led
LED Name                 LED State  LED Color
------------------------ ---------- --------
LED_SYS_ACT              OFF        GREEN
LED_HLTH_STATUS          ON         GREEN

Server /chassis #  show led detail
LEDs:
    LED Name: LED_SYS_ACT
```

```
    LED State: OFF
    LED Color: GREEN
LEDs:
    LED Name: LED_HLTH_STATUS
    LED State: ON
    LED Color: GREEN
ucs-e160dp-m1 /chassis #
```

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。 次のステータスがあります。 [HDD*X*_PRS]：各ハード ドライブの有無を示します。
[Status] カラム	ストレージ デバイスのステータスの簡単な説明。
[LED Status] カラム	現在の LED の色（ある場合）。 ストレージ デバイスの物理 LED を点滅させるには、ドロップダウン リストから [Turn On] を選択します。 LED の点滅をストレージ デバイスに制御させるには、[Turn Off] を選択します。

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
-------------------- --------------------
HDD1_PRS             inserted
HDD2_PRS             inserted
HDD3_PRS             inserted

Server /chassis #
```

第 7 章

リモート プレゼンスの管理

この章は、次の内容で構成されています。

- 仮想 KVM の管理，83 ページ
- 仮想メディアの設定，86 ページ
- Serial over LAN の管理，87 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

KVM コンソールを使用して、サーバにオペレーティング システムまたはハイパーバイザをインストールし、次の作業を行うことができます。

- 起動中に F2 を押して、BIOS セットアップ メニューにアクセスします。
- 起動中に F8 を押して、CIMC 設定ユーティリティにアクセスします。
- 起動中に Ctrl キーと H キーを押して WebBIOS にアクセスし、RAID を設定します。

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。
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 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。

	コマンドまたはアクション	目的
		（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 encrypted** {**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 encrypted 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 リダイレクション
- フロー制御なし

- ボー レートを SoL と同様に設定
- VT-100 terminal type
- レガシー OS リダイレクションをディセーブル

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オペレーティング システム（OS）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

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。
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 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

Ctrl キーと X キーを押して SoL から切断し、CLI セッションに戻ります。

（注） SoL をイネーブルにすると、シリアル ポートからの出力がリダイレクトされます。このため、Cisco IOS CLI を使用してホストのセッションに入ろうとすると、出力は表示されません。

第 8 章

ユーザ アカウントの管理

この章は、次の内容で構成されています。

- ローカル ユーザの設定，91 ページ
- Active Directory，92 ページ
- ユーザ セッションの表示，96 ページ
- ユーザ セッションの終了，96 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

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

Active Directory サーバにカスタム属性を作成するには、次の手順を実行します。

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

手順

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

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

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

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

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

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

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

Active Directory（AD）サーバを使用してローカル ユーザを認証および許可する場合は、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。
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 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 4	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 5	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。

	コマンドまたはアクション	目的
ステップ 6	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 7	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 8	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 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 #
```

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。 たとえば、CLI、vKVM などです。
[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 9 章

ネットワーク関連の設定

この章は、次の内容で構成されています。

- CIMC NIC の設定，99 ページ
- 共通プロパティの設定，102 ページ
- IPv4 の設定，102 ページ
- サーバ VLAN の設定，104 ページ
- ネットワーク セキュリティの設定，105 ページ

CIMC NIC の設定

CIMC NIC

CIMC への接続には、2 種類の NIC モードを使用できます。

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。

- 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、マザーボードのオンボード LAN（LOM）イーサネット ホスト ポート経由およびルータの PCIe と MGF インターフェイス経由で使用できます。

（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。

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-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。

CIMC NIC の設定

NIC モードと NIC 冗長化を設定するには、次の手順を実行します。

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** | **shared_lom**}	NIC モードを次のいずれかに設定します。 • 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 へのアクセスにマザーボードのオンボード LAN（LOM）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。
ステップ 4	Server /cimc/network # **set redundancy** {**none** | **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。

	コマンドまたはアクション	目的
		• 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 # **set interface** {**console** | **ge1** | **ge2** | **ge3** | **ge1-ge2** | **ge1-ge3** | **ge2-ge3** | **ge1-ge2-ge3**}	NIC インターフェイスを、次のいずれかに設定します。 • console：ルータの PCIe インターフェイスを E シリーズ サーバ に接続するために使用される内部インターフェイス。 • ge1：高速バックプレーン スイッチで CIMC にアクセスするために使用される内部インターフェイス。 • ge2：プライマリ インターフェイスまたはバックアップ インターフェイスとして使用できる外部インターフェイス。 • ge3：プライマリ インターフェイスまたはバックアップ インターフェイスとして使用できる外部インターフェイス。 • ge1-ge2：GE1 インターフェイスと GE2 インターフェイスの間のフェールオーバー（アクティブ スタンバイのみ）。 • ge1-ge3：GE1 インターフェイスと GE3 インターフェイスの間のフェールオーバー（アクティブ スタンバイのみ）。 • ge2-ge3：GE2 インターフェイスと GE3 インターフェイスの間のフェールオーバー（アクティブ スタンバイのみ）。 • ge1-ge2-ge3：GE1 インターフェイス、GE2 インターフェイス、および GE3 インターフェイスの間のフェールオーバー（アクティブ スタンバイのみ）。 （注） GE3 インターフェイスに関連するすべてのインターフェイス オプションは、ダブルワイド E シリーズ サーバだけに適用できます。
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。 （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。
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 no
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: no
    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。
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 10 章

コミュニケーション サービスの設定

この章は、次の内容で構成されています。

- HTTP の設定，107 ページ
- SSH の設定，108 ページ
- XML API の設定，109 ページ
- IPMI の設定，110 ページ
- SNMP の設定，112 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 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 6	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 timeout 1800
Server /http *# commit
Server /http # show
HTTP Port  HTTPS Port Timeout  Active Sessions Enabled
---------- ---------- -------- --------------- -------
80         443        1800     0               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。 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。

	コマンドまたはアクション	目的
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 の XML API

Cisco CIMC XML アプリケーション プログラム インターフェイス（API）は、E シリーズ サーバの CIMC へのプログラマチック 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 に関する詳細については、『*CCIMC XML API Programmer's Guide for Cisco UCS E-Series Servers*』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。
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。

	コマンドまたはアクション	目的
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
```

IPMI の設定

IPMI over LAN

インテリジェント プラットフォーム管理インターフェイス（IPMI）では、サーバ プラットフォームに組み込まれているサービス プロセッサとのインターフェイスのためのプロトコルを定義しています。 このサービス プロセッサはベースボード管理コントローラ（BMC）と呼ばれ、サーバのマザーボードに存在します。 BMC は、メイン プロセッサおよびボード上の他の要素に、簡単なシリアル バスを使用してリンクします。

通常動作の間、IPMI は、サーバのオペレーティング システムがシステム ヘルスについての情報を取得し、システムのハードウェアを制御できるようにします。 たとえば、IPMI を使用すると、温度、ファンの速度、および電圧などのセンサーをモニタして、問題を事前に検出できます。 サーバの温度が指定されているレベルより高くなった場合、サーバのオペレーティング システムは BMC に対して、ファンの速度を上げたり、プロセッサの速度を下げたりして問題に対処するよう指示できます。

IPMI over LAN の設定

IPMI over LAN は、CIMC を IPMI メッセージで管理する場合に設定します。

はじめる前に

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

手順

	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 E-Series Servers 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。

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。

	コマンドまたはアクション	目的
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, （113 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 権限を持つユーザとし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**}	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。

	コマンドまたはアクション	目的
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 2
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
```

テスト SNMP トラップ メッセージの送信

はじめる前に

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

手順

	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。

	コマンドまたはアクション	目的
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。 次のいずれかが可能です。 • **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。

	コマンドまたはアクション	目的
		（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 ユーザ名を設定します。
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 レベルを設定します。次のいずれかになります。 • **noauthnopriv**：ユーザは、許可パスワードとプライバシー パスワードのいずれも必要としません。 • **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設定します。
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設定します。
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設定します。
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）を設定します。
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: ******
```

第 11 章

証明書の管理

この章は、次の内容で構成されています。

- サーバ証明書の管理，119 ページ
- 証明書署名要求の生成，120 ページ
- 自己署名証明書の作成，121 ページ
- サーバ証明書のアップロード，123 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**	証明書署名要求（CSR）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。

- 公共の認証局からの証明書の取得を望んでおらず、組織が独自の認証局を運用していない場合は、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、アップロードするという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** 例： `# openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 04`	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
	-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

この章は、次の内容で構成されています。

- プラットフォーム イベント フィルタ，125 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，126 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，126 ページ
- プラットフォーム イベント フィルタの設定，127 ページ
- プラットフォーム イベント トラップの解釈，128 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、アクションをトリガーしたり、ハードウェア関連の重要なイベントが発生したときは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
Platform Event Enabled
----------------------
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
Platform Event Enabled
----------------------
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	プロセッサ アサート フィルタ
5	メモリ緊急アサート フィルタ
6	ドライブ スロット アサート フィルタ
7	LSI 緊急アサート フィルタ
8	LSI 警告アサート フィルタ

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。

	コマンドまたはアクション	目的
		• **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 1
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
--------------------- ------------------------------------- ----------- -----------
1                     Temperature Critical 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

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
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]

イベント番号 [注記 1]		プラットフォーム イベントの説明
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
884489	0D7F09h	ドライブ スロット低下

（注） 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、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

ファームウェアの管理

この章は、次の内容で構成されています。

- ファームウェアの概要，131 ページ
- Cisco Systems からファームウェアを取得するためのオプション，132 ページ
- シスコからのソフトウェアの取得，132 ページ
- リモート サーバからの CIMC ファームウェアのインストール，134 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，135 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，137 ページ

ファームウェアの概要

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

起こりうる問題を回避するため、Host Upgrade Utility（HUU）を使用することを強く推奨します。このユーティリティは、CIMC、BIOS、およびその他のファームウェア コンポーネントを互換性のあるレベルにアップグレードします。 このユーティリティに関する詳細については、http://www.cisco.com/en/US/products/ps12629/prod_installation_guides_list.html にある『*Host Upgrade Utility User Guide for Cisco UCS E-Series Servers*』を参照してください。 このマニュアルには、互換性のある HUU、CIMC、および BIOS ソフトウェア リリースに関する情報も記載されています。

（注） HUU は、CIMC のリリース 2.1.0 以降のリリースでサポートされています。

CIMC および BIOS ファームウェアを（HUU を使用する代わりに）手動でアップグレードする場合は、最初に CIMC ファームウェアを更新してから、BIOS ファームウェアを更新します。 互換性のある CIMC ファームウェアをアクティブ化するまでは、新しい BIOS ファームウェアをインストールしないでください。インストールすると、サーバが起動しなくなります。

CIMC ファームウェアの更新プロセスは、次の段階に分けられます。これは、サーバがオフラインになる時間を最小限にするためです。

- インストール：この段階では、CIMC は、選択した CIMC ファームウェアをサーバの非アクティブまたはバックアップ スロットにインストールします。
- アクティブ化：この段階では、CIMC は、非アクティブ ファームウェア バージョンをアクティブとして設定してサーバをリブートします。これにより、サービスが中断されます。サーバをリブートすると、新規のアクティブ スロット内のファームウェアが、実行中のバージョンになります。

CIMC ファームウェアをアクティブ化した後は、BIOS ファームウェアを更新できます。 BIOS 更新プロセス全体にわたって、サーバの電源をオフにしておく必要があります。 CIMC がリブートを完了すると、サーバの電源をオンにして、サービスに戻すことができます。

（注） 古いファームウェア バージョンを新しいものにアップグレードしたり、新しいファームウェア バージョンを古いものにダウングレードしたりできます。

Cisco Systems からファームウェアを取得するためのオプション

- HUU ISO ファイルを使用して、すべてのファームウェア コンポーネントをアップグレードすることを推奨します。これらのコンポーネントには、BIOS および CIMC ファームウェアが含まれています。 HUU を使用してファームウェアをアップグレードする手順の詳細については、http://www.cisco.com/en/US/products/ps12629/prod_installation_guides_list.html にある『*Host Upgrade Utility User Guide for Cisco UCS E-Series Servers*』の「Upgrading the Firmware Using the HUU」の項を参照してください。

  （注） HUU は、CIMC のリリース 2.1.0 以降のリリースでサポートされています。

- CIMC および BIOS ファームウェアを手動でアップグレードする場合は、シスコからのソフトウェアの取得, （132 ページ）を参照してください。

シスコからのソフトウェアの取得

ドライバ、BIOS と CIMC のファームウェア、および診断イメージをダウンロードするには、次の手順を実行します。

手順

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

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

ステップ 3 上部にあるメニュー バーで、[Support] をクリックします。
ロールダウン メニューが表示されます。

ステップ 4 [Downloads]（中央）ペインから、[All Downloads]（右下隅）をクリックします。
[Download Software] ページが表示されます。

ステップ 5 左ペインから、[Products] をクリックします。

ステップ 6 中央ペインから、[Unified Computing and Servers] をクリックします。

ステップ 7 右ペインから、[Cisco UCS E-Series Software] をクリックします。

ステップ 8 右ペインから、ダウンロードするソフトウェアのサーバ モデルの名前をクリックします。
次のカテゴリを含む [Download Software] ページが表示されます。

- [Unified Computing System (UCSE) Server Drivers]：ドライバが含まれています。
- [Unified Computing System (UCSE) Server Firmware]：Host Upgrade Utility と、BIOS および CIMC ファームウェアのイメージが含まれています。
- [Unified Computing System (UCSE) Utilites]：診断イメージが含まれています。

ステップ 9 適切なソフトウェア カテゴリ リンクをクリックします。

ステップ 10 ダウンロードするソフトウェア イメージに関連付けられている [Download] ボタンをクリックします。
[End User License Agreement] ダイアログボックスが表示されます。

ステップ 11 （任意）複数のソフトウェア イメージをダウンロードするには、次を実行します。

a) ダウンロードするソフトウェア イメージに関連付けられている [Add to cart] ボタンをクリックします。

b) 右上にある [Download Cart] ボタンをクリックします。
カートに追加したすべてのイメージが表示されます。

c) 右下隅にある [Download All] をクリックして、すべてのイメージをダウンロードします。
[End User License Agreement] ダイアログボックスが表示されます。

ステップ 12 [Accept License Agreement] をクリックします。

ステップ 13 必要に応じて、次のいずれかを実行します。

- ソフトウェア イメージ ファイルをローカル ドライブに保存します。
- ソフトウェア イメージを TFTP サーバからインストールする場合は、使用する TFTP サーバにファイルをコピーします。

サーバは、TFTP サーバ上の宛先フォルダに対して読み取り権限を持っている必要があります。

次の作業

ソフトウェア イメージをインストールします。

リモートサーバからのCIMCファームウェアのインストール

（注） 起こりうる問題を回避するため、Host Upgrade Utility（HUU）を使用することを強く推奨します。このユーティリティは、CIMC、BIOS、およびその他のファームウェア コンポーネントを互換性のあるレベルにアップグレードします。 このユーティリティに関する詳細については、http://www.cisco.com/en/US/products/ps12629/prod_installation_guides_list.html にある『*Host Upgrade Utility User Guide for Cisco UCS E-Series Servers*』を参照してください。 このマニュアルには、互換性のある HUU、CIMC、および BIOS ソフトウェア リリースに関する情報も記載されています。

CIMC および BIOS ファームウェアを（HUU を使用する代わりに）手動でアップグレードする場合は、最初に CIMC ファームウェアを更新してから、BIOS ファームウェアを更新します。互換性のある CIMC ファームウェアをアクティブ化するまでは、新しい BIOS ファームウェアをインストールしないでください。インストールすると、サーバが起動しなくなります。

はじめる前に

- admin 権限を持つユーザとして CIMC にログインします。
- シスコから CIMC ファームウェア ファイルを取得します。 シスコからのソフトウェアの取得, （132 ページ）を参照してください。

（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。

	コマンドまたはアクション	目的
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** *protocol ip-address path*	プロトコル、リモート サーバの IP アドレス、サーバ上のファームウェア ファイルへのファイル パスを指定します。 プロトコルは次のいずれかになります。 • tftp • ftp • sftp • scp • http
ステップ 4	（任意）Server /cimc # **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、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 tftp 10.20.34.56 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 #
```

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。

重要　アクティブ化の進行中は、次のことを行わないでください。

- サーバのリセット、電源切断、シャットダウン。
- CIMC のリブートまたはリセット。
- 他のすべてのファームウェアをアクティブ化します。
- テクニカル サポート データまたは設定データをエクスポートします。

（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。

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 # **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 3	Server /cimc # **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 # 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 # 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） 起こりうる問題を回避するため、Host Upgrade Utility（HUU）を使用することを強く推奨します。このユーティリティは、CIMC、BIOS、およびその他のファームウェア コンポーネントを互換性のあるレベルにアップグレードします。 このユーティリティに関する詳細については、http://www.cisco.com/en/US/products/ps12629/prod_installation_guides_list.html にある『*Host Upgrade Utility User Guide for Cisco UCS E-Series Servers*』を参照してください。 このマニュアルには、互換性のある HUU、CIMC、および BIOS ソフトウェア リリースに関する情報も記載されています。

CIMC および BIOS ファームウェアを（HUU を使用する代わりに）手動でアップグレードする場合は、最初に CIMC ファームウェアを更新してから、BIOS ファームウェアを更新します。互換性のある CIMC ファームウェアをアクティブ化するまでは、新しい BIOS ファームウェアをインストールしないでください。インストールすると、サーバが起動しなくなります。

はじめる前に

シスコから CIMC ファームウェア ファイルを取得します。 シスコからのソフトウェアの取得, （132 ページ）を参照してください。

（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。
ステップ 3	（任意）Server /bios # **show detail**	BIOS 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、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 10.20.34.56 //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 /bios #
```

第 14 章

ログの表示

この章は、次の内容で構成されています。

- CIMC ログ，139 ページ
- System Event Log，143 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                 Source           Description
-------------------- ---------------- ---------------------------------------
1970 Jan 4 18:55:36 BMC:kernel:-
<7>/build/trunk/bmc/drivers/pilot2_i2c/pilot2_i2c.c:306:I2c Controller-4 DAT is stuck-low,
 issuing One Clock Pulse.
1970 Jan 4 18:55:36 BMC:kernel:-
```

```
<7>/build/trunk/bmc/drivers/pilot2_i2c/pilot2_i2c.c:301:I2c Controller-4 Loop:[0].
1970 Jan 4 18:55:36 BMC:kernel:-     "
<7>/build/trunk/bmc/drivers/pilot2_i2c/pilot2_i2c.c:422: Controller-4 has a stuck bus,
attempting to clear it now... "
1970 Jan 4 18:55:36 BMC:kernel:-     "
<7>/build/trunk/bmc/drivers/pilot2_i2c/pilot2_i2c.c:402: Controller-4 Initiating I2c recovery
 sequence. "
1970 Jan 4 18:55:36 BMC:IPMI:480     last message repeated 22 times
1970 Jan 4 18:55:28 BMC:IPMI:480     "  mcddI2CDrv.c:850:PI2CWriteRead: ioctl to driver
failed to read Bus[f4].Dev[5e]! ErrorStatus[77] "
1970 Jan 4 18:55:33 BMC:IPMI:486     last message repeated 17 times
1970 Jan 4 18:55:28 BMC:IPMI:486     "  mcddI2CDrv.c:850:PI2CWriteRead: ioctl to driver
failed to read Bus[f4].Dev[b0]! ErrorStatus[77] "
1970 Jan 4 18:55:31 BMC:IPMI:486     last message repeated 17 times
1970 Jan 4 18:55:26 BMC:IPMI:486     "  mcddI2CDrv.c:850:PI2CWriteRead: ioctl to driver
failed to read Bus[f4].Dev[b2]! ErrorStatus[77] "
1970 Jan 4 18:55:26 BMC:kernel:-
<7>/build/trunk/bmc/drivers/pilot2_i2c/pilot2_i2c.c:306:I2c Controller-4 DAT is stuck-low,
 issuing One Clock Pulse.
1970 Jan 4 18:55:26 BMC:kernel:-
<7>/build/trunk/bmc/drivers/pilot2_i2c/pilot2_i2c.c:301:I2c Controller-4 Loop:[8].
--More--
```

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。

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 # **scope server** {**1** | **2**}	2 つのリモート syslog サーバ プロファイルのうち 1 つを選択し、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 4	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 5	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 6	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、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 # 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 #
```

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**	システム イベント ログ（SEL）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。**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。
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

この章は、次の内容で構成されています。

- リモート サーバへのテクニカル サポート データのエクスポート，145 ページ
- CIMC の再起動，147 ページ
- CIMC の出荷時デフォルトへのリセット，148 ページ
- CIMC 設定のエクスポートとインポート，149 ページ

リモート サーバへのテクニカル サポート データのエクスポート

このタスクは、Cisco Technical Assistance Center（TAC）から要求された場合に実行します。 このユーティリティは、TAC が技術上の問題をトラブルシューティングおよび解決する際に役立つ設定情報、ログ、および診断データが含まれる要約レポートを作成します。

手順

	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。
ステップ 3	Server /cimc/tech-support # **set remote-ip** *ip-address*	サポート データ ファイルを保存する必要のあるリモート 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 remote-path** *path/filename*	サーバ上に保存するサポート データのファイル名を指定します。 この名前を入力するときは、

	コマンドまたはアクション	目的
		ファイルの相対パスを、サーバ ツリーの最上位から目的の場所まで含めてください。
ステップ 5	Server /cimc/tech-support # **set remote-protocol** *protocol-type*	リモート サーバ プロトコルを指定します。 リモート サーバ プロトコルは、次のいずれかです。 • tftp • ftp • sftp • scp • http
ステップ 6	Server /cimc/tech-support # **set remote-username** *username*	（任意）システムがリモート サーバへのログインに使用する必要のあるユーザ名。 （注） このユーザ名は、リモート サーバが TFTP または HTTP の場合は適用されません。
ステップ 7	Server /cimc/tech-support # **set remote-password** *password*	（任意）リモート ユーザ名のパスワード。 （注） このパスワードは、リモート サーバが TFTP または HTTP の場合は適用されません。
ステップ 8	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 9	Server /cimc/tech-support # **start**	リモート サーバへのサポート データ ファイルの転送を開始します。
ステップ 10	Server /cimc/tech-support # **show detail**	ファイルのアップロードのステータスを表示します。
ステップ 11	Server /cimc/tech-support # **cancel**	（任意）リモート サーバへのサポート データ ファイルの転送を取り消します。

次に、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 remote-ip 10.20.30.41
Server /cimc/tech-support *# set remote-path /user/user1/supportfile
Server /cimc/tech-support *# set remote-protocol tftp
Server /cimc/tech-support *# commit
Server /cimc/tech-support # start
```

```
 Tech Support upload started.
Server /cimc/tech-support # show detail
Tech Support:
    Server Address: 10.20.30.41
    Path: /user/user1/supportfile
    Protocol: tftp
    Username:
    Password: ******
    Progress(%): 0
    Status: COLLECTING
Server /cimc/tech-support # show detail
Tech Support:
    Server Address: 10.20.30.41
    Path: /user/user1/supportfile
    Protocol: tftp
    Username:
    Password: ******
    Progress(%): 85
    Status: COLLECTING
Server /cimc/tech-support # show detail
Tech Support:
    Server Address: 10.20.30.41
    Path: /user/user1/supportfile
    Protocol: tftp
    Username:
    Password: ******
    Progress(%): 100
    Status: COMPLETED
```

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**	確認のプロンプトが表示されたら、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
This operation will reboot the CIMC.
Continue?[y|N]y
```

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。
- 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 です）。
- 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。

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 ファイルのインポート時に SNMP の設定情報を復元する場合は、コンフィギュレーション ファイルを作成する前に、このサーバで SNMP がイネーブルになっていることを確認します。 コンフィギュレーションをエクスポートするときに SNMP がディセーブルになっていると、CIMC は、ファイルのインポート時に SNMP の値を適用しません。

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 # **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

はじめる前に

コンフィギュレーション ファイルのインポート時に SNMP 設定情報を復元する場合は、インポートを行う前にこのサーバで SNMP がディセーブルになっていることを確認します。 インポート時に SNMP がイネーブルになっていると、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

	コマンドまたはアクション	目的
		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 #
```

第 16 章

診断テスト

この章は、次の内容で構成されています。

- 診断テストの概要，153 ページ
- ホストへの診断イメージのマッピング，154 ページ
- 診断テストの実行，155 ページ

診断テストの概要

診断テストはEシリーズサーバ上で実行されるスタンドアロンユーティリティで、同サーバで動作するオペレーティングシステムやアプリケーションからは独立しています。 Eシリーズサーバで問題が発生した場合、診断テストを使用して事前チェックを実行し、問題点を特定することができます。 診断テストはサーバの CPU、メモリ、およびブロック デバイスで実行できます。 ブロック デバイスにはハード ドライブ、USB ドライブ、SD カードなどがあります。

診断テストに合格した場合、サーバのCPU、メモリ、ブロックデバイスに問題はありません。 他のハードウェア コンポーネントまたはソフトウェア設定に問題がある可能性があります。 http://www.cisco.com/cisco/web/support/index.html の Cisco Technical Assistance Center（TAC）でサービス要求を開始し、問題点を特定してください。

診断テストが失敗した場合は、Cisco TAC でサービス要求を開いて支援を求めます。

注意 診断テストは非破壊テストですが、テストの実行中に停電または機器の故障が発生した場合、ディスクデータが破損することがあります。 診断テストを実行する前に、データをバックアップしておくことを強く推奨します。

診断テストを実行するための基本的なワークフロー

1 データをバックアップします。

2 E シリーズ サーバには、購入時に診断イメージが事前にインストールされています。 最新の診断イメージを、指定した FTP または HTTP サーバから CIMC 内部リポジトリにダウンロードすることもできます。

3 診断イメージを USB コントローラの HDD 仮想ドライブにマウントします。

4 EFI シェルが最初のブート デバイスになるように、ブート順を設定します。

5 サーバをリブートします。

6 EFI シェルから診断テストを実行します。

7 仮想メディアのブート順を元の設定にリセットします。

ホストへの診断イメージのマッピング

はじめる前に

- データをバックアップします。
- admin 権限を持つユーザとして CIMC にログインします。
- E シリーズ サーバには、購入時に診断イメージが事前にインストールされています。 最新の診断イメージを、指定した FTP、FTPS、HTTP、または HTTPS サーバから CIMC 内部リポジトリにダウンロードすることもできます。 「シスコからのソフトウェアの取得」を参照してください。

（注） アップデートがすでに処理中であるときにイメージ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 remote-install**	remote install コマンド モードを開始します。
ステップ 2	Server /remote-install # **download-image** {**ftp** | **ftps** | **http** | **https**} *server-ip-address path / filename* [**username** *username* **password** *password*]	指定したリモート サーバから CIMC 内部リポジトリにイメージをダウンロードします。 診断イメージのファイル拡張子は必ず .diag になります。 リモート サーバには、FTP、FTPS、HTTP、または HTTPS サーバを指定できます。 リモート サーバでユーザ認証が必要な場合は、リモート サーバのユーザ名とパスワードを追加する必要があります。

	コマンドまたはアクション	目的
		（注） イメージ ファイルがサイズ制限を超えると、エラー メッセージが表示されます。
ステップ 3	（任意）Server /remote-install # **show detail**	診断イメージダウンロードのステータスを表示します。
ステップ 4	Server /remote-install # **map-diagnostics**	USB コントローラの HDD 仮想ドライブにイメージをマウントします。
ステップ 5	（任意）Server /remote-install # **show detail**	診断イメージマッピングのステータスを表示します。

次に、診断イメージをマッピングする例を示します。

```
Server# scope remote-install
Server /remote-install # download-image ftp 10.20.34.56 pub/diagnostics-image.diag
---
Server /remote-install # show detail
Host Image Info:
  Name: DiagnosticsImage.diag
  Size: 6626848
  Last Modified Time: Fri, 12 Aug 2011 21:13:27 GMT
  Host Image Status: Download Successful!!
Server /remote-install # map-diagnostics
---
status: ok
---
Server /remote-install # show detail
Host Image Info:
  Name: DiagnosticsImage.diag
  Size: 6626848
  Last Modified Time: Fri, 12 Aug 2011 21:13:27 GMT
  Host Image Status: Image mapped successfully!!
```

次の作業

1 EFI シェルが最初のブート デバイスになるように、ブート順を設定します。

2 サーバをリブートします。 EFI シェルが表示されます。

3 診断テストを実行します。

診断テストの実行

EFI シェルから、次の手順を使用して診断テストを実行します。

はじめる前に

- バック アップ データ。 テストはすべて非破壊的ですが、テストの実行中に停電や装置の障害が発生すると、ディスク データが破損する可能性があります。 これらのテストを実行する前に、データをバックアップしておくことを強く推奨します。

- CIMC CLI または CIMC GUI を使用して、診断イメージをダウンロードし、USB コントローラの HDD 仮想ドライブ上にマップします。
- サーバをリブートします。 EFI シェルが表示されます。

手順

	コマンドまたはアクション	目的
ステップ 1	Shell > **dir** *virtual-media-drive-name***:**	指定した仮想メディア ドライブ内に存在するすべてのファイル パッケージを表示します。 ドライブ名は fs0 から始まり、fs0、fs1、fs2 などがあります。 （注） 仮想メディア ドライブ名の末尾に必ずコロンを追加してください。 例：dir fs1:
ステップ 2	Shell > *virtual-media-drive-name***:**	診断ファイルが保存されている仮想メディア ドライブに移動します。
ステップ 3	Virtual Media Drive :\> **cp** *package-file-name* **dsh.pkg**	診断を実行するパッケージ ファイルを診断シェル パッケージ ファイルにコピーします。
ステップ 4	Virtual Media Drive :\> **dsh**	診断シェルを開始します。 確認プロンプトで、y と答えます。
ステップ 5	Server: SRV > **run all**	使用可能なすべての診断テストを実行し、テストの進行状況とステータスを表示します。 診断テストは、サーバの CPU、メモリ、およびブロック デバイス上で実行されます。 ブロック デバイスにはハード ドライブ、USB ドライブ、SD カードなどがあります。 サーバ上で特定の診断テストを実行するには、run *test-name* コマンドを使用します。 *test-name* には次のいずれかを指定できます。 • cpux64：CPU の診断テスト。 • diskx64：ブロック デバイスの診断テスト。 ブロック デバイスにはハード ドライブ、USB ドライブ、SD カードなどがあります。 • memoryx64：メモリの診断テスト。 （注） 診断テストの実行には、約 10 分の時間がかかる可能性があります。
ステップ 6	（任意）Server: SRV > **results**	テスト ステータスが Passed または Failed の診断テストのサマリーを表示します。

	コマンドまたはアクション	目的
		（注） このサマリー レポートは、失敗および合格したテストの数を示します。 どのテストが失敗または合格したかについての情報は提供しません。 失敗および合格したテストを判別するには、run all コマンドの出力を確認してください。
ステップ 7	（任意）Server: SRV > **show**	サーバ上で管理されていたグローバルパラメータと診断テスト モジュールの一覧を表示します。
ステップ 8	Server: SRV > **exit**	診断シェルを終了します。
ステップ 9	Cisco TAC でサービス要求を開きます。	診断テストに合格した場合、サーバの CPU、メモリ、ブロック デバイスに問題はありません。 他のハードウェア コンポーネントまたはソフトウェア設定に問題がある可能性があります。 Cisco TAC でサービス要求を開いて、問題を特定します。 診断テストが失敗した場合は、Cisco TAC でサービス要求を開いて支援を求めます。

次の例では、すべての診断テストを実行しています。

```
Shell > dir fs1:
  06/27/12  07:48p            1,435,424  Dsh.efi
  06/27/12  08:03p               10,036  dsh-e140d.pkg
  06/25/12  06:00p               10,140  dsh-e140s.pkg
  06/27/12  08:04p               10,042  dsh-e160d.pkg
          4 File(s)   1,465,642 bytes
Shell > fs1:
fs1:\> cp dsh-e140d.pkg dsh.pkg
copying fs0:\OBD\dsh-e140d.pkg -> fs0:\OBD\dsh.pkg
- [ok]
fs1:\> dsh
Diagnostics is a standalone utility that runs on the server module independent
of the operating system or applications running on the module.All tests are
non-destructive, but there is a possibility of disk datacorruption during
power or equipment failure when the tests are in progress. Therefore, before
executing these tests, we highly recommend that you backup the data.


For questions or concerns with this utility, please open a Service Request
with Cisco TAC at http://www.cisco.com/cisco/web/support/index.html

(Y)es to continue test. (N)o to exit(y/n): Y
Cisco Diagnostics  Shell 1.03(0.3) Thu 06/28/-16:35:08.95-canis-diag@cisco.com
UCS-E140D-M1/K9:SRV>

Server: SRV > run all
Server: SRV > results
Test Name          : all
Test Status        : Passed
Failed/Run History : 0/17
Start Time         : 06/27/12 14:38:19
End Time           : 06/27/12 14:43:36
Diag Version       : 1.03(0.3) Mon 04/02/-17:07:57.19-canis-diag@cisco.com
Board S/N          : FOC160724BY
```

```
Server: SRV > show
Server: SRV > exit
```

次の作業

仮想メディアのブート順を元の設定にリセットします。

索 引

A

Active Directory 92, 93, 94
  CIMC の設定 94

B

BIOS 31, 32, 132, 137
  CMOS 31
    クリア 31
  シスコからのファームウェアの取得 132
  シスコからのファームウェアの取得オプション 132
  パスワード 32
    クリア 32
  ファームウェア 137
    TFTP サーバからのインストール 137
BIOS CMOS 31
  クリア 31
BIOS ステータス 29
  表示 29
BIOS 設定 29, 30, 32, 33
  高度な 29
  概要 33
  サーバ管理 30
  デフォルトの復元 32
BIOS パスワード 32
  クリア 32
BIOS ファームウェア 137
  TFTP サーバからのインストール 137

C

CIMC 69, 131, 132, 134, 135, 139, 140, 142, 148
  出荷時の初期状態へのリセット 148
  ファームウェア 134, 135
    アクティブ化 135
CIMC (続き)
  ファームウェア (続き)
    リモート サーバからのインストール 134
  ファームウェアの概要 131
  ファームウェアの詳細 69
  ログしきい値の設定 140
  ログのクリア 140
  ログの送信 142
  ログの表示 139
CIMC CLI 3
CIMC NIC 99
CIMC の概要 2
CIMC ファームウェア 135
  アクティブ化 135
CIMC ファームウェアの詳細 69
  表示 69
CPU プロパティ 69

E

E シリーズ サーバ 1
  概要 1

H

HTTP プロパティ 107

I

IOS CLI 設定のロック 22
IOS CLI 設定のロック解除 23
IPMI over LAN 110
  説明 110
IPMI over LAN プロパティ 110
IPv4 プロパティ 102

IP ブロッキング 105

K

KVM 84, 85
　イネーブル化 84, 85
　設定 84
　ディセーブル化 85
KVM コンソール 12, 83
KVM のイネーブル化 84, 85
KVM のディセーブル化 85

L

LDAP。参照先： Active Directory
LED センサー 81
LOM ポート 77
　プロパティの表示 77

M

MAC アドレス 77
　インターフェイス 77

N

NIC プロパティ 100

O

OS のインストール 11, 13
　PXE 13
　方法 11

P

PCI アダプタ 75
　プロパティの表示 75
PXE インストール 12

R

RAID 49, 52
　削除 52
　設定 49
RAID オプション 45

S

Serial over LAN 87, 88, 89
　起動 89
　設定 88
SNMP 112, 113, 114, 115
　SNMPv3 ユーザの設定 115
　テスト メッセージの送信 114
　トラップ設定の指定 113
　プロパティの設定 112
SSH プロパティ 108
syslog 142
　CIMC ログの送信 142

V

VLAN プロパティ 104
VMware 18
　ソフトウェアの取得 18

X

XML API 109
　イネーブル化 109
　説明 109

Y

YAML 8

あ

アダプタ 75
　PCI 75

い

イベント 126
　プラットフォーム 126
　　アラートのイネーブル化 126
　　アラートのディセーブル化 126
イベント フィルタ、プラットフォーム 125, 127
　概要 125
　設定 127
イベント ログ、システム 143, 144
　クリア 144
　表示 143
インポート 150
　CIMC 設定 150

え

エクスポート 149
　CIMC 設定 149

お

温度センサー 80

か

仮想 KVM 84, 85
仮想ドライブ 58, 60, 63
　再構築 63
　再構築のオプション 60
　整合性検査の実行 58
仮想メディア 86
仮想メディアの暗号化 86

き

共通プロパティ 102

こ

コミュニケーション サービスのプロパティ 107, 108, 110
　HTTP プロパティ 107
　IPMI over LAN プロパティ 110
コミュニケーション サービスのプロパティ *(続き)*
　SSH プロパティ 108

さ

サーバ管理 19, 21, 22, 24, 25, 26
　サーバ電源の再投入 26
　サーバのシャットダウン 22
　サーバの電源オフ 25
　サーバの電源投入 24
　サーバのリセット 21
　ブート順の設定 19
サーバ証明書のアップロード 123
サーバ ソフトウェア 1
サーバ電源の再投入 26
サーバのシャットダウン 22
サーバの電源オフ 25
サーバの電源投入 24
サーバの電源ボタンのロック 26
サーバの電源ボタンのロック解除 27
サーバのプロパティ 67
サーバのリセット 21
削除 17, 58

し

自己署名証明書 121
システム イベント ログ 143, 144
　クリア 144
　表示 143
自動再構築、イネーブル化 57
障害 79
　サマリーの表示 79
障害サマリー 79
　表示 79
証明書管理 123
　証明書のアップロード 123
診断 155
　テスト、実行 155
診断イメージ 154

す

ストレージ センサー 82
　表示 82

ストレージのプロパティ 71, 73, 74
アダプタのプロパティの表示 71
仮想ドライブのプロパティの表示 74
物理ドライブのプロパティの表示 73

せ

設定 149, 150
インポート 150
エクスポート 149
バックアップ 149
センサー 80
温度 80
電圧 80

そ

ソフトウェア 18
VMware からの取得 18

て

テクニカル サポート データ、エクスポート 145
電圧センサー 80
電源のプロパティ 71
電源ポリシーの統計情報 76
表示 76

ね

ネットワーク セキュリティ 105
ネットワーク接続 78
status 78
ネットワーク プロパティ 100, 102, 104
IPv4 プロパティ 102
NIC プロパティ 100
VLAN プロパティ 104
共通プロパティ 102

は

ハード ドライブのプレゼンス 76
バックアップ 149
CIMC 設定 149

ふ

ファームウェア 131, 132, 134
概要 131
シスコからの取得 132
リモート サーバからのインストール 134
ファームウェア オプション 132
シスコからの取得 132
ブート可能なディスク ドライブ 64
CIMC CLI の使用 64
ブート順 68
表示 68
ブート順、設定 19
物理ドライブ 54, 55
再構築 54
削除 55
物理ドライブの状態 53
変更 53
プラットフォーム イベント 126, 128
アラートのイネーブル化 126
アラートのディセーブル化 126
トラップの解釈 128
プラットフォーム イベント フィルタ 125, 127
概要 125
設定 127
フロッピーディスクのエミュレーション 86

ほ

ホスト イメージ 13, 14, 16, 17
ホストへのマッピング 154

ま

マッピング 13, 14
マッピング解除 16

め

メモリのプロパティ 70

ゆ

ユーザ管理 91, 94, 96
Active Directory 94
終了、ユーザ セッション 96
ユーザ セッションの表示 96
ローカル ユーザ 91
ユーザ セッション 96
終了 96
表示 96

り

リモート プレゼンス 84, 85, 86, 88, 89
Serial over LAN の起動 89
Serial over LAN の設定 88
仮想 KVM 84, 85
仮想メディア 86
リンク ステート 78

ろ

ローカル ユーザ 91