Cisco UCS E シリーズ サーバ Integrated Management Controller の CLI 設定ガイド リリース 1.0

初版：2012 年 09 月 07 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-26443-01-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。

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

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

© 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

関連資料 xii

マニュアルに関するフィードバック xiii

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 2

CIMC の概要 3

CIMC CLI 4

コマンド モード 4

コマンド モード表 5

コマンドの完了または終了 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 11

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

ホストのイメージ マッピング 13
ホストのイメージのマッピング 14
Microsoft Windows Server でのドライバのインストール 16
ホストのイメージのマッピング解除 16
ホストのイメージの削除 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 20
サーバのシャットダウン 21
サーバの電源の管理 21
サーバの電源投入 21
サーバの電源オフ 22
サーバ電源の再投入 23
RAID の管理 23
RAID オプション 23
RAID の設定 27
ディスク ドライブのブート可能化 30
RAID 設定の変更 32
ストレージ コントローラでの自動再構築のイネーブル化 32
仮想ドライブの整合性検査の実行 32
仮想ドライブ オプションの再構築 34
仮想ドライブの再構築 36
RAID 設定の削除 38
物理ドライブの状態の変更 39
物理ドライブの再構築 40
BIOS の設定 41
BIOS ステータスの表示 41
TFTP サーバからの BIOS ファームウェアのインストール 42
高度な BIOS の設定 43
サーバ管理 BIOS の設定 44
BIOS CMOS のクリア 44

BIOS パスワードのクリア 45
BIOS デフォルトの復元 45
サーバ BIOS 設定 46
サーバのプロパティの表示 59
サーバのプロパティの表示 59
CPU のプロパティの表示 60
メモリのプロパティの表示 60
電源のプロパティの表示 62
ストレージのプロパティの表示 62
ストレージ アダプタのプロパティの表示 62
物理ドライブのプロパティの表示 64
仮想ドライブのプロパティの表示 65
PCI アダプタのプロパティの表示 66
電源ポリシーの統計情報の表示 67
ハード ドライブのプレゼンスの表示 67
サーバのセンサーの表示 69
障害の要約の表示 69
温度センサーの表示 70
電圧センサーの表示 70
ストレージ センサーの表示 71
リモート プレゼンスの管理 73
仮想 KVM の管理 73
KVM コンソール 73
仮想 KVM の設定 74
仮想 KVM のイネーブル化 75
仮想 KVM のディセーブル化 75
仮想メディアの設定 76
Serial Over LAN の管理 77
Serial Over LAN 77
Serial Over LAN に関するガイドラインおよび制約事項 77
Serial over LAN の設定 78
Serial Over LAN の起動 79

ユーザ アカウントの管理 81

ローカル ユーザの設定 **81**

Active Directory **82**

Active Directory サーバの設定 **83**

CIMC での Active Directory の設定 **84**

ユーザ セッションの表示 **86**

ユーザ セッションの終了 **86**

ネットワーク関連の設定 89

CIMC NIC の設定 **89**

CIMC NIC **89**

CIMC NIC の設定 **90**

共通プロパティの設定 **92**

IPv4 の設定 **92**

サーバ VLAN の設定 **94**

ネットワーク セキュリティの設定 **95**

ネットワーク セキュリティ **95**

ネットワーク セキュリティの設定 **95**

コミュニケーション サービスの設定 97

HTTP の設定 **97**

SSH の設定 **98**

IPMI の設定 **99**

IPMI Over LAN **99**

IPMI over LAN の設定 **99**

SNMP の設定 **101**

SNMP **101**

SNMP プロパティの設定 **101**

SNMP トラップ設定の指定 **102**

テスト SNMP トラップ メッセージの送信 **103**

証明書の管理 105

サーバ証明書の管理 **105**

証明書署名要求の生成 **106**

自己署名証明書の作成 **107**

サーバ証明書のアップロード **109**

プラットフォーム イベント フィルタの設定 111
プラットフォーム イベント フィルタ 111
プラットフォーム イベント アラートのイネーブル化 111
プラットフォーム イベント アラートのディセーブル化 112
プラットフォーム イベント フィルタの設定 113
CIMC ファームウェア管理 115
CIMC ファームウェアの概要 115
シスコからのソフトウェアの取得 116
TFTP サーバからの CIMC ファームウェアのインストール 118
インストールされている CIMC ファームウェアのアクティブ化 119
CIMC 情報の表示 119
ログの表示 121
CIMC ログ 121
CIMC ログの表示 121
CIMC ログのクリア 122
リモート サーバへの CIMC ログの送信 122
システム イベント ログ 124
システム イベント ログの表示 124
システム イベント ログのクリア 125
サーバ ユーティリティ 127
テクニカル サポート データのエクスポート 127
CIMC の再起動 128
CIMC の出荷時デフォルトへのリセット 129
CIMC コンフィギュレーションのエクスポートおよびインポート 130
CIMC コンフィギュレーションのエクスポートおよびインポート 130
CIMC コンフィギュレーションのエクスポート 131
CIMC コンフィギュレーションのインポート 132
診断テスト 133
診断テストの概要 133
ホストへの診断イメージのマッピング 134
診断テストの実行 135

はじめに

この前書きは、次の項で構成されています。

- 対象読者，ix ページ
- マニュアルの構成，ix ページ
- 表記法，xi ページ
- 関連資料，xii ページ
- マニュアルに関するフィードバック，xiii ページ

対象読者

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

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

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 および 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	サーバのオペレーティング システム（OS）を設定する方法について説明します。
第 3 章	サーバの管理	サーバのブート デバイスの順序を設定する方法、サーバの電源を管理する方法、電源ポリシーを設定する方法、RAID を設定および管理する方法、BIOS 設定を構成する方法について説明します。
第 4 章	サーバのプロパティの表示	サーバの CPU、メモリ、電源、ストレージ、および PCI アダプタのプロパティを表示する方法について説明します。
第 5 章	サーバのセンサーの表示	障害、温度、電圧、ストレージのセンサーの表示方法について説明します。
第 6 章	リモート プレゼンスの管理	仮想 KVM、仮想メディア、および Serial over LAN 接続の設定方法を説明します。
第 7 章	ユーザ アカウントの管理	ユーザ アカウントを追加または変更する方法、ユーザを認証するように Active Directory を設定する方法、ユーザ セッションを管理する方法について説明します。
第 8 章	ネットワーク関連の設定	ネットワーク インターフェイス、ネットワーク設定、およびネットワーク セキュリティの設定方法を説明します。
第 9 章	コミュニケーション サービスの設定	HTTP、SSH、IPMI、および SNMP によってサーバ管理コミュニケーションを設定する方法について説明します。
第 10 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 11 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について説明します。
第 12 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 13 章	ログの表示	CIMC およびシステムのイベント ログ メッセージを表示、エクスポート、クリアする方法について説明します。

章	タイトル	説明
第 14 章	サーバ ユーティリティ	サポート データをエクスポートする方法、サーバの設定をエクスポートおよびインポートする方法、出荷時の初期状態にサーバの設定をリセットする方法、管理インターフェイスをリブートする方法について説明します。
第 15 章	診断テスト	診断テストを実行する方法について説明します。

表記法

このマニュアルでは、次の表記法を使用しています。

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

関連資料

- 『Documentation Guide for Cisco UCS E-Series Servers』：E シリーズ サーバの全マニュアルへのリンクを提供します。
- 『*Release Notes for Cisco UCS E-Series Servers, Release 1.0*』
- 『*Getting Started Guide for Cisco UCS E-Series Servers, Release 1.0*』
- 『*Hardware Installation Guide for Cisco UCS E-Series Servers*』
- 『*Cisco Network Modules, Server Modules, and Interface Cards Regulatory Compliance and Safety Information*』
- 『*GUI Configuration Guide for Cisco UCS E-Series Servers Integrated Management Controller, Release 1.0*』
- 『*CLI Configuration Guide for Cisco UCS E-Series Servers Integrated Management Controller, Release 1.0*』
- 『*Troubleshooting Guide for Cisco UCS E-Series Servers*』
- 『*Open Source Used in Cisco UCS E-Series Servers, Release 1.0*』

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，2 ページ
- CIMC の概要，3 ページ
- CIMC CLI，4 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 Cisco UCS Express サーバの次世代です。 E シリーズ サーバ ファミリは、サイズ、重量、および電力の効率が高いブレード サーバで、第 2 世代 Cisco Integrated Services Router（ISR G2）内に格納されます。 これらのサーバは、Microsoft Windows や Linux などのオペレーティング システム上にベアメタルとして、または VMware vSphere Hypervisor™、Microsoft Hyper-V、Citrix XenServer などのハイパーバイザ上に仮想マシンとして展開されるブランチ オフィス アプリケーション用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。

E シリーズ サーバは、Cisco 2900 シリーズまたは 3900 シリーズ ISR G2 に置かれます。 次の E シリーズ サーバがサポートされます。

- UCS-E140S：シングル幅 E シリーズ サーバ
- UCS-E140D：倍幅 E シリーズ サーバ、4 コア CPU
- UCS-E160D：倍幅 E シリーズ サーバ、6 コア CPU
- UCS-E140DP：倍幅 E シリーズ サーバ、4 コア CPU、PCIe
- UCS-E160DP：倍幅 E シリーズ サーバ、6 コア CPU、PCIe

（注） 各 ISR G2 ごとにインストールできる E シリーズ サーバの最大数については、『*Getting Started Guide for Cisco UCS E-Series Servers*』の「Server Hardware」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）はマザーボードに組み込まれている独立した管理モジュールです。 専用の ARM ベースのプロセッサが、メイン サーバ CPU とは別に、CIMC ファームウェアを実行します。 システムには CIMC ファームウェアの実行バージョンが付属しています。 CIMC ファームウェアは更新できますが、初期インストールは必要ではありません。

CIMC は E シリーズ サーバ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 はシステムのハードウェアを初期化し、ブート可能デバイスを検出し、これらを指定された手順でブートします。 オペレーティング システムをブートし、使用するオペレーティング システム用にハードウェアを設定します。 BIOS 管理機能によって、ハードウェアと対話して使用することができます。 また、BIOS はシステムを設定し、ファームウェアを管理し、BIOS のエラーレポートを作成するためのオプションを提供します。

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

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 Microsoft Windows や Linux などのオペレーティング システム上で、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。

次のプラットフォームは E シリーズ サーバでテスト済みです。

- Microsoft Windows：
  - Windows Server 2008 R2 Standard 64 ビット
  - Windows Server 2008 R2 Enterprise 64 ビット

- Linux の場合
  - Red Hat Enterprise Linux 6.2
  - SUSE Linux Enterprise 11 Service Pack 2
  - Oracle Enterprise Linux 6.0 Update 2
- ハイパーバイザ：
  - VMware vSphere Hypervisor™ 5.0 Update 1
  - Hyper-V（Windows 2008 R2）
  - Citrix XenServer 6.0

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 アカウントの作成と管理、および Active Directory を介したリモート ユーザ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
- サーバ障害が発生したときにテクニカル 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インターフェイスまたはCLIインターフェイスで実行でき、一方のインターフェイスで実行されたタスクの結果は、もう一方にも表示されます。 ただし、次の操作はできません。

- CIMC GUI を使用して CIMC CLI を呼び出すことはできません
- CIMC CLI で呼び出したコマンドは CIMC GUI では表示できません
- CIMC GUI から CIMC CLI の出力を生成することはできません

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は次のように起動できます。

- シリアル ポートから。
- SSH を通じてネットワークで。
- **ucse** *slot* **session imc** コマンドを使用して、ルータから。

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

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 同じスコープ内で行われた変更を保存するために、**commit** コマンドを使用する必要があります。 **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，11 ページ
- PXE インストール サーバ，12 ページ
- ホストのイメージ 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シリーズサーバは、複数のオペレーティング システムとハイパーバイザをサポートします。インストールされているプラットフォームに関係なく、次のいずれかのツールを使用してサーバにインストールできます。

- KVM コンソール
- PXE インストール サーバ
- Host Image Mapping

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）
- コンピュータの USB フラッシュ ドライブ

KVM コンソールを使用して、オペレーティング システムまたはハイパーバイザをサーバにインストールし、次を実行できます。

- ブートアップ中に F2 キーを押して、BIOS セットアップ メニューにアクセスします。
- ブートアップ中に F8 キーを押して、CIMC Configuration Utility にアクセスします。
- ブートアップ中に 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 ロケーション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し、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、LAN（通常は専用のプロビジョニング LAN）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、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ために、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できます。 また、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ために、独自のディスク イメージを使用できます。

（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™ に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」を参照してください。

手順

ステップ 1 PXE のブート順を設定します。

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。

ホストのイメージ マッピング

ホストのイメージマッピング機能を使用して、ホストのイメージをダウンロード、マッピング、マッピング解除、または削除することができます。 Microsoft Windows、Linux、または VMware などのホストのイメージを、リモート側の 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し、E シリーズ サーバ の USB コントローラの仮想ドライブにイメージをマッピングします。 イメージをマッピングした後、イメージがマウントされる仮想デバ

イス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 .iso である必要があります。

ホストのイメージ マッピング機能を使用して、診断イメージをダウンロードし、マウントすることができます。 診断イメージのファイル拡張子は .diag である必要があります。

ホストの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のイメージ ファイルを取得します。

（注） VMware vSphere Hypervisor™ に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」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の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 .iso である必要があります。 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。
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。 仮想ドライブは次のいずれかになります。

	コマンドまたはアクション	目的
		• 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

次の操作を行います。

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」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。 イメージをインストールするには、ウィザードの手順に従います。
3. オペレーティング システムまたはハイパーバイザのインストール後にディスク ドライブが表示されない場合、ドライバをインストールする必要があります。 Microsoft Windows Server にドライバをインストールする方法については、「Microsoft Windows Server でのドライバのインストール」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 で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（プレインストールされたオペレーティング システムまたはハイパーバイザのない E シリーズ サーバ）を購入し、Microsoft Windows Server の独自のバージョンをインストールする場合は、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 つ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

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」を参照してください。

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

ステップ 3 Microsoft Windows Server の独自のバージョンをインストールします。
インストール プロセス中に、LSI ドライバの入力を求められます。

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。

ホストの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	（任意）Server /remote-install # **show detail**	ホストのイメージのマッピング解除に関する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!!
```

ホストのイメージの削除

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

VMware vSpere Hypervisor™ のカスタマイズされたイメージをダウンロードするには、次の手順を使用します。

手順

ステップ 1 https://my.vmware.com/web/vmware/login に移動します。
[VMware login] ページが表示されます。

ステップ 2 VMware の資格情報を入力し、[Log In] をクリックします。
VMware のアカウントを持っていない場合は、[Register] をクリックし、無料アカウントを作成してください。

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

ステップ 4 右上隅にある [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、VMware vSpere Hypervisor™ のカスタマイズされたイメージをダウンロードします。

次の作業

VMware vSpere Hypervisor™ の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、「ホストの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，20 ページ
- サーバのシャットダウン，21 ページ
- サーバの電源の管理，21 ページ
- RAID の管理，23 ページ
- BIOS の設定，41 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

次の作業を実行するには、user または admin 権限でログインする必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope bios**	bios コマンド モードを開始します。
ステップ 2	Server /bios # **set boot-order** *device1*[,*device2*[,*device3*[,*device4*[,*device5*]]]]	ブート デバイス オプションと順序を指定します。次の 1 つ以上を選択できます。 • cdrom：ブート可能 CD-ROM

	コマンドまたはアクション	目的
		• fdd：フロッピーディスク ドライブ • hdd：ハードディスク ドライブ • pxe：PXE ブート • efi：Extensible Firmware Interface
ステップ 3	Server /bios # **commit**	トランザクションをシステムの設定にコミットします。

新規のブート順は、次の BIOS のブートで使用されます。

次に、ブート順を設定し、トランザクションをコミットする例を示します。

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

Server /bios #
```

サーバのリセット

はじめる前に

次の作業を実行するには、user または admin 権限でログインする必要があります。

手順

	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

次の作業を実行するには、user または admin 権限でログインする必要があります。

手順

	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
```

サーバの電源の管理

サーバの電源投入

（注） サーバの電源がCIMC経由以外の何らかの方法でオフにされた場合、サーバは電源をオンにしてもすぐにはアクティブになりません。 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

次の作業を実行するには、user または admin 権限でログインする必要があります。

手順

	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

次の作業を実行するには、user または admin 権限でログインする必要があります。

手順

	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

次の作業を実行するには、user または admin 権限でログインする必要があります。

手順

	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
```

RAID の管理

RAID オプション

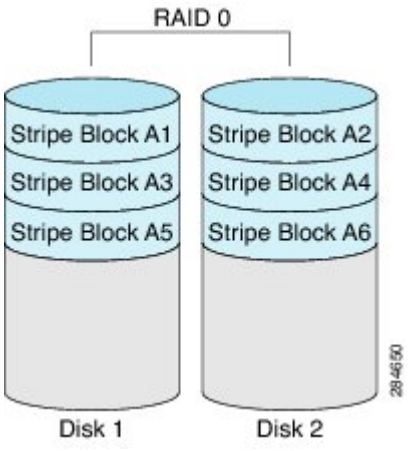
E シリーズ サーバのデータ ファイルをローカルの Redundant Array of Inexpensive Disks（RAID）に保存できます。 次の RAID レベルがサポートされます。

- シングル幅の E シリーズ サーバは、RAID 0 および RAID 1 レベルをサポートします。
- 倍幅の E シリーズ サーバは、RAID 0、RAID 1、および RAID 5 レベルをサポートします。
- PCIe オプションを搭載した倍幅の E シリーズ サーバは、RAID 0 および RAID 1 レベルをサポートします。

RAID 0

RAID 0 を使用している場合、データは冗長性（ミラーリング）なしで 1 台以上のディスク ドライブにストライプ ブロックで均等に保存されます。 ディスク ドライブすべてのデータが異なります。

図 *1*：*RAID 0*



データを保存するためにディスク ドライブの両方が使用されているため、RAID 1 と比較して、RAID 0 では追加のストレージが提供されます。 パフォーマンスは、読み取りおよび書き込み操作が 2 台のディスク ドライブ内で並行して発生するため向上します。

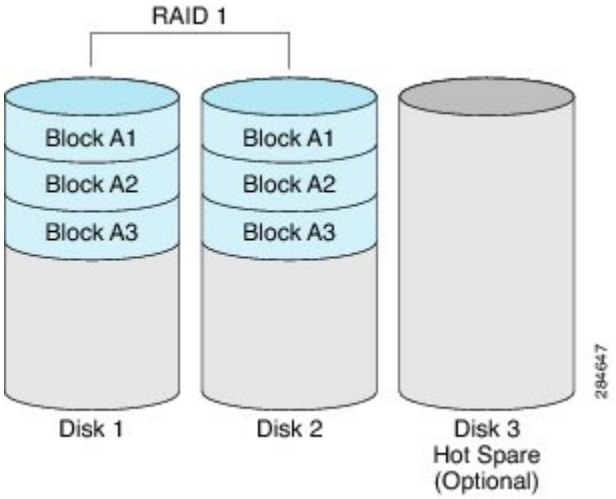
ただし、耐障害性、エラー チェック、ホット スペア、またはホット スワップはありません。 一方のディスク ドライブで障害が発生した場合は、アレイ全体のデータが破壊されます。 エラー チェックやホットスワップの機能がないため、アレイは回復不能なエラーの影響を受けやすくなります。

RAID 1

RAID 1 は、ディスク ドライブの両方でデータが同一であるミラーリングされた一連のディスク ドライブを作成し、冗長性とハイ アベイラビリティを提供します。 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 ドライブも使用できます。 ホット スペア ドライブは常にアクティブで、フェールオーバー時のホット スタンバイ ドライブとして準備状態のまま保持されます。

図 *2*：*RAID 1*



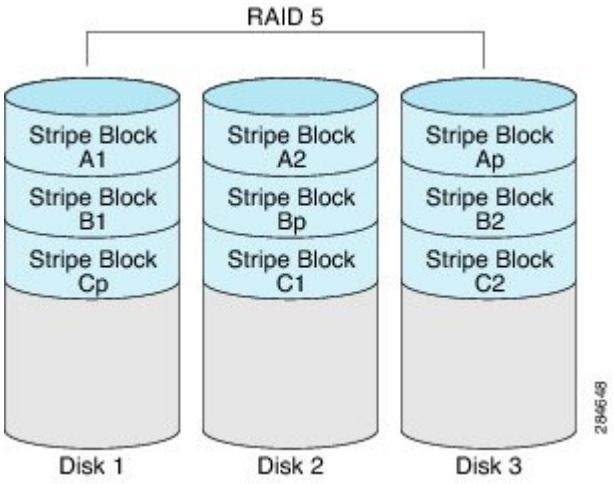
RAID 1 は、耐障害性とホット スワップをサポートします。 1 台のディスク ドライブで障害が発生した場合は、障害のあるディスク ドライブを取り外して新しいディスク ドライブに交換することができます。

ただし、ストレージに使用できるのは使用可能な合計ディスク領域の半分だけなので、RAID 0 と比較して格納域が少なく、パフォーマンスにも影響があります。

RAID 5

RAID 5 を使用している場合、データはすべてのディスク ドライブでパリティ データをずらしたストライプ ブロックで保存され、低コストで冗長性が提供されます。

図 *3* : *RAID 5*



RAID 5 は RAID 1 を超えるデータ ストレージ容量と、RAID 0 より優れたデータ保護を提供します。 また、ホット スワップをサポートします。ただし、RAID 1 の方が高いパフォーマンスを提供します。

非 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、または冗長性をサポートしていません。

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で均等に保存されたデータ	• より大きなストレージ • 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	ミラーリングされたディスク ドライブおよび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	• 少ないストレージ • パフォーマンス上の影響
RAID 5	すべてのディスク ドライブで、パリティ データをずらしたストライプ ブロックで保存されたデータ	• RAID 1 より優れたストレージ効率 • RAID 0 より優れた耐障害性 • 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 用に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

RAID レベル、ストリップのサイズ、ホスト アクセス権限、ドライブのキャッシュ、および初期化パラメータを仮想ドライブに設定するには、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-***slot-number*	インストールされているストレージ カードのコマンド 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 ◦ 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。 ◦ 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。 • （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。

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-***slot-number*	インストールされているストレージ カードのコマンド 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。

	コマンドまたはアクション	目的
		（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：ドライブは、ドライブ グループまたはホット スペア プールに割り当てられる準備が整っています。 ドライブにモードは設定されていません。 • hotspare：ドライブはスペア ドライブとして指定されています。 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
```

RAID 設定の変更

ストレージ コントローラ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、この手順を実行します。 RAID を使用して設定されたディスク ドライブの 1 つの機能が低下し、新しいドライブがそれに接続されると、新しいドライブ上で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-***slot-number*	インストールされているストレージ カードのコマンド 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-***slot-number*	インストールされているストレージカードのコマンド モードを開始します。
ステップ 4	Server /chassis/storageadapter # **scope virtual-drive** *drive-number*	指定し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 # **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 オプションの再構築

新しい RAID レベルに仮想ドライブを移行（再構築）するには、物理ドライブを追加または削除する必要があります。 物理ドライブを追加または削除すると、仮想ドライブのサイズは保持されるか増加します。

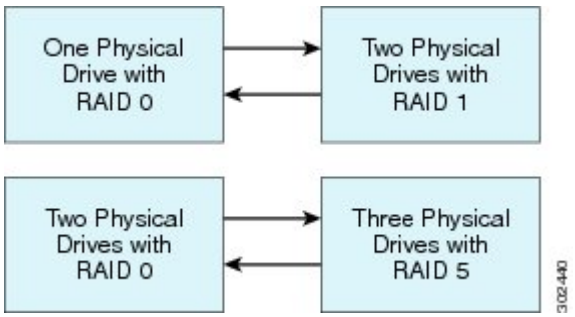
仮想ドライブのサイズを保持することも増やすこともできますが、サイズを小さくすることはできません。 たとえば、RAID 0 で 2 台の物理ドライブがある場合、同じドライブ数の RAID 1 には移行できません。 RAID 1 はミラーリングされた一連のディスク ドライブを作成するため、RAID 0 から RAID 1 への移行によって仮想ドライブのサイズが減少しますが、これはサポートされません。

注意 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。 再構築プロセス中にシステムを使用し続けることができます。

仮想ドライブのサイズを保持するオプション

新しい RAID レベルに仮想ドライブを移行するときに仮想ドライブのサイズを保持するオプションについては、次の図とその後の表を参照してください。

図 *4*：仮想ドライブのサイズを保持するオプション



次の表では、仮想ドライブのサイズを保持するオプションのリストを示し、特定の RAID レベルに仮想ドライブを移行するために追加または取り外しが必要な物理ドライブの数についての情報を提供します。

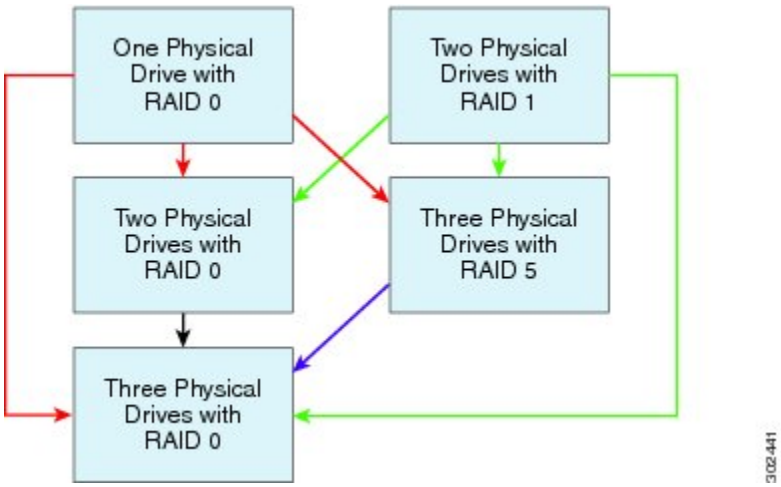
表 *1*：仮想ドライブのサイズを保持

変更前：	移行先	ディスクの追加または取り外し
RAID 0 で 1 台の物理ドライブ	RAID 1 で 2 台の物理ドライブ	1 台のディスクを追加します。
RAID 1 で 2 台の物理ドライブ	RAID 0 で 1 台の物理ドライブ	1 台のディスクを取り外します。
RAID 0 で 2 台の物理ドライブ	RAID 5 で 3 台の物理ドライブ	1 台のディスクを追加します。
RAID 5 で 3 台の物理ドライブ	RAID 0 で 2 台の物理ドライブ	1 台のディスクを取り外します。

仮想ドライブのサイズを増加させるオプション

新しいRAID レベルに仮想ドライブを移行するときに仮想ドライブのサイズを増加させるオプションについては、次の図とその後の表を参照してください。

図 *5*：仮想ドライブのサイズを増加させるオプション



次の表では、仮想ドライブのサイズを増加させるオプションのリストを示し、特定の RAID レベルに仮想ドライブを移行するために追加または取り外しが必要な物理ドライブの数についての情報を提供します。

表 *2*：仮想ドライブのサイズを増加

変更前：	移行先	ディスクの追加または取り外し
RAID 0 で 1 台の物理ドライブ 図の赤い矢印を参照してください。	RAID 0 で 2 台の物理ドライブ	1 台のディスクを追加します。
	RAID 5 で 3 台の物理ドライブ	2 台のディスクを追加します。
	RAID 0 で 3 台の物理ドライブ	2 台のディスクを追加します。
RAID 1 で 2 台の物理ドライブ 図の緑色の矢印を参照してください。	RAID 0 で 2 台の物理ドライブ	—
	RAID 5 で 3 台の物理ドライブ	1 台のディスクを追加します。
	RAID 0 で 3 台の物理ドライブ	1 台のディスクを追加します。
RAID 0 で 2 台の物理ドライブ 図の黒い矢印を参照してください。	RAID 0 で 3 台の物理ドライブ	1 台のディスクを追加します。
RAID 5 で 3 台の物理ドライブ 図の紫色の矢印を参照してください。	RAID 0 で 3 台の物理ドライブ	—

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 オプションの再構築」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。

	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-***slot-number*	インストールされているストレージ カードのコマンド モードを開始します。
ステップ 4	Server /chassis/storageadapter # **scope virtual-drive** *drive-number*	指定し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。
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
```

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-***slot-number*	インストールされているストレージカードのコマンド 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 などのオプションがあります。

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 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-***slot-number*	インストールされているストレージ カードのコマンド 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*	指定し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 などのオプションがあります。
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

手動で物理ドライブの再構築プロセスを開始するには、この手順を使用します。

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-***slot-number*	インストールされているストレージカードのコマンド 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*	指定し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。

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
```

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 のステータスの詳細を表示します。

BIOS の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 ストリング。
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リカバリ アクションのステータス。

名前	説明
FW Update/Recovery Progress	最新のファームウェア アップデートまたはリカバリ アクションの完了率。

次に、BIOS の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 #
```

TFTP サーバからの BIOS ファームウェアのインストール

はじめる前に

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

高度な BIOS の設定

（注） インストール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コンフィギュレーション オプションは表示されないことがあります。

はじめる前に

次の作業を実行するには、admin 権限でログインする必要があります。

手順

	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**	advanced BIOS 設定のコマンド モードを開始します。
ステップ 3	BIOS 設定値を設定します。	CLI コマンドに関する各 BIOS 設定のオプションの詳細については、次のトピックを参照してください。 • 高度な設定：プロセッサの BIOS 設定, （46 ページ） • 高度な設定：メモリの BIOS 設定, （54 ページ） • 高度な設定：シリアル ポートの BIOS 設定, （54 ページ） • 高度な設定：USB BIOS 設定, （54 ページ）
ステップ 4	Server /bios/advanced # **commit**	トランザクションをシステムの設定にコミットします。 変更は次のサーバのリブート時に適用されます。 サーバの電源がオンの場合、すぐにリブートするかどうかを選択するように求められます。

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

次の作業を実行するには、admin 権限でログインする必要があります。

手順

	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**	BIOS の server management コンフィギュレーション コマンド モードを開始します。
ステップ 3	BIOS 設定値を設定します。	CLI コマンドに関する各 BIOS 設定のオプションの詳細については、次のトピックを参照してください。 • サーバ管理 BIOS 設定, （55 ページ）
ステップ 4	Server /bios/server-management # **commit**	トランザクションをシステムの設定にコミットします。 変更は次のサーバのリブート時に適用されます。サーバの電源がオンの場合、すぐにリブートするかどうかを選択するように求められます。

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。

次に、BIOS のデフォルト設定を復元する例を示します。

```
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

次のセクションの表に、表示および設定ができるサーバの BIOS 設定のリストを示します。

各設定について、CLI **set** コマンドが表の設定名の下に表示され、コマンドオプションは設定の説明に記載されています。 各設定のデフォルトを表示するには、後ろに疑問符を付けた **set** コマンドを入力します。 表示されるオプションキーワードで、デフォルトのオプションがアスタリスクでマークされます。

（注） サーバの BIOS 設定のサポートを確認することを推奨します。 インストール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ない場合があります。

高度な設定：プロセッサの 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]：プロセッサは自動的に周波数を上げません。 • [Enabled]：必要に応じてプロセッサで Turbo Boost Technology が利用されます。

名前	説明
[Enhanced Intel Speedstep Technology] **set EnhancedIntelSpeedStep**	プロセッサで Enhanced Intel SpeedStep Technology を使用するかどうか。これにより、システムでは、プロセッサ電圧とコア周波数を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]：プロセッサは、電圧または周波数を動的に調整しません。 • [Enabled]：プロセッサは、拡張版インテル SpeedStep テクノロジーを利用し、電力をさらに節約するために、サポートされているすべてのプロセッサ スリープ状態をイネーブルにします。 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お薦めします。
[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お薦めします。

名前	説明
[Number of Enabled Cores] **set CoreMultiProcessing**	パッケージの論理プロセッサ コアの状態を設定します。この設定をディセーブルにした場合、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 コアの多重処理をイネーブルにします。 • [1] から [n] ：サーバで実行可能な論理プロセッサ コアの数を指定します。 多重処理をディセーブルにして、サーバで実行される論理プロセッサ コアを 1 個のみにするには、[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お薦めします。
[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。 この分類の結果として、プロセッサでは、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ときに、コードを実行できないようにします。 この設定は、損傷、ワーム感染、および特定のクラスの悪意のあるバッファ オーバーフロー攻撃を防ぐのに役立ちます。 次のいずれかになります。 • [Disabled]：プロセッサはメモリ領域を分類しません。 • [Enabled]：プロセッサはメモリ領域を分類します。 オペレーティング システムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることをお薦めします。

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]：プロセッサでのバーチャライゼーションを禁止します。 • [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**	プロセッサで Intel Virtualization Technology for Directed I/O（VT-d）を使用するかどうか。 次のいずれかになります。 • [Disabled]：プロセッサでバーチャライゼーションテクノロジーを使用しません。 • [Enabled]：プロセッサでバーチャライゼーションテクノロジーを使用します。
[Intel VT-d Interrupt Remapping] **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**	プロセッサが I/O デバイスからのデータをプロセッサのキャッシュに直接配置することによって I/O パフォーマンスを向上できるようにします。 この設定は、キャッシュ ミスを削減するのに役立ちます。 次のいずれかになります。 • [Disabled]：I/O デバイスからのデータは、プロセッサのキャッシュに直接配置されません。 • [Enabled]：I/O デバイスからのデータは、プロセッサのキャッシュに直接配置されます。
[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を決定します。 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]：ACPI 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]：ACPI 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を決定します。 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、メモリからデータ ストリームおよび命令を統合型 L2 キャッシュに読み込む際に、必要に応じて、Intel のハードウェア プリフェッチャを使用できるかどうか。 次のいずれかになります。 • [Disabled]：ハードウェア プリフェッチャは使用されません。 • [Enabled]：プロセッサは、キャッシュの問題を検出した場合にハードウェア プリフェッチャを使用します。 （注） この値を指定するには、[CPU Performance] の設定で [Custom] を選択する必要があります。[Custom] 以外の値の場合、このオプションは選択した CPU パフォーマンス プロファイルの設定で上書きされます。

名前	説明
[Package C State Limit] **set PackageCstateLimit**	アイドル状態である場合に使用可能なサーバ コンポーネントへの電力量。 次のいずれかになります。 • [C0_state]：サーバが全電力をすべてのサーバ コンポーネントに常に提供します。 このオプションは、パフォーマンスの最高レベルを維持し、最大の電力量を必要とします。 • [C2_state]：システム レベルの調整が進行中で、結果として電力消費が高くなります。 調整が完了するまでパフォーマンスの問題がある可能性があります。 • [C6_state]：CPU がアイドル状態の場合、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削減します。 このオプションは、C0 または C2 よりも多くの電力を節約しますが、サーバがハイ パフォーマンス モードに戻るまでにパフォーマンス上の問題がある可能性があります。 • [C7_state]：CPU がアイドル状態のときに、サーバでは、最小限の電力をコンポーネントで使用できるようにします。 このオプションは、節約される電力の量は最大になりますが、サーバがハイ パフォーマンス モードに戻るまで最も長い時間を必要とします。 • [No_Limit]：サーバは、使用可能な任意の C 状態になれます。 （注） このオプションは、[CPU C State] がイネーブルの場合にだけ使用されます。

名前	説明
[Patrol Scrub] **set PatrolScrub**	サーバのメモリの未使用部分であっても、単一ビットのメモリ エラーをシステムでアクティブに検索して訂正するかどうか。 次のいずれかになります。 • [Disabled]：システムでは、CPU がメモリ アドレスを読み取るか書き込む場合のみ、メモリ ECC エラーをチェックします。 • [Enabled]：システムでは、定期的にメモリの読み取りと書き込みを行って ECC エラーを検索します。エラーが検出された場合、修正を試みます。 このオプションにより、複数ビット エラーになる前に 1 ビット エラーを修正できる可能性がありますが、パトロール スクラビング処理が実行されている場合、パフォーマンスに悪影響を与える可能性があります。
[Demand Scrub] **set DemandScrub**	オンデマンドでメモリのスクラビング処理を実行できるようにするかどうか。 次のいずれかになります。 • [Disabled]：システムは、オンデマンドでメモリのスクラビング処理を実行することを許可しません。 • [Enabled]：オンデマンドでメモリのスクラビング処理を実行できます。 エラーが検出された場合、システムは修正を試みるか、読み込めないというマークを付けます。 このプロセスによって、システムは高速で実行でき、データ処理エラーが少なくなります。
[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]：システムはデバイスとインターフェイスのグループ化を許可しません。 • [Enabled]：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ます。

高度な設定：メモリの **BIOS** 設定

名前	説明
[Select Memory RAS] **set SelectMemoryRAS**	サーバでメモリのRAS（信頼性、可用性、有用性）がどのように設定されるか。 次のいずれかになります。 • [Maximum_Performance]：システム 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]：ミラーリングよりも多くのメモリがオペレーティングシステムで使用できると同時に、ある程度のメモリの冗長性によりシステムの信頼性が拡張されます。

高度な設定：シリアル ポートの **BIOS** 設定

名前	説明
[Serial A Enable] **set Serial-PortA**	シリアルポートAがイネーブルまたはディセーブルのどちらに設定されているか。 次のいずれかになります。 • [Disabled]：シリアル ポートはディセーブルです。 • [Enabled]：シリアル ポートはイネーブルです。

高度な設定：**USB BIOS** 設定

名前	説明
[USB Port 0] **set USBPort0**	プロセッサが 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]：サーバは USB ポート 0 を使用しません。 • [Enabled]：プロセッサは USB ポート 0 を使用します。
[USB Port 1] **set USBPort1**	プロセッサが 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]：サーバは USB ポート 1 を使用しません。 • [Enabled]：プロセッサは 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）が発生した場合に BIOS でマスク不可能割り込み（NMI）を生成し、エラーを記録するかどうか。 次のいずれかになります。 • [Disabled]：BIOS は SERR が発生したときに NMI を生成せず、エラーを記録しません。 • [Enabled]：BIOS は SERR が発生すると NMI を生成し、エラーを記録します。 [Assert NMI on PERR] をイネーブルにするには、この設定をイネーブルにする必要があります。
[Assert NMI on PERR] **set AssertNMIOnPERR**	プロセッサのバス パリティ エラー（PERR）が発生した場合に BIOS でマスク不可能割り込み（NMI）を生成し、エラーを記録するかどうか。 次のいずれかになります。 • [Disabled]：BIOS は PERR が発生したときに NMI を生成せず、エラーを記録しません。 • [Enabled]：BIOS は PERR が発生すると NMI を生成し、エラーを記録します。 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 中にシステムが停止した場合に、システムを回復するために CIMC で FRB2 タイマーを使用するかどうか。 次のいずれかになります。 • [Disabled]：FRB2 タイマーは使用されません。 • [Enabled]：POST 中に FRB2 タイマーが開始され、システムを必要に応じて回復するために使用されます。

名前	説明
[Console Redirection] **set ConsoleRedir**	POST 中と 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 がブートし、オペレーティング システムがサーバを制御するようになれば、コンソール リダイレクションは無関係になり、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と、同時に、POST 中の [Quiet Boot] ロゴ画面の表示がディセーブルになります。
[Flow Control] **set FlowCtrl**	フロー制御にハンドシェイク プロトコルを使用するかどうか。送信要求/クリア ツー センド（RTS/CTS）は非表示端末の問題によって発生することがあるフレームの衝突を削減するのに役立ちます。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]：フロー制御に RTS/CTS が使用されます。 （注） この設定は、リモート ターミナル アプリケーション上の設定と一致する必要があります。

名前	説明
[Baud Rate] **set BaudRate**	シリアル ポート伝送速度にいずれのボー レートを使用するか。 コンソール リダイレクションをディセーブルにした場合、このオプションは使用できません。 次のいずれかになります。 • [9.6k]：ボー レート 9600 が使用されます。 • [19.2k]：ボー レート 19200 が使用されます。 • [38.4k]：ボー レート 38400 が使用されます。 • [57.6k]：ボー レート 57600 が使用されます。 • [115.2k]：ボー レート 115200 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する必要があります。
[Terminal Type] **set TerminalType**	どのような文字フォーマットがコンソール リダイレクションに使用されるか。 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 VT-100 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 文字セット対応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する必要があります。

名前	説明
[OS Boot Watchdog Timer] **set OSBootWatchdogTimer**	BIOS が指定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。 タイマーが期限切れになる前にオペレーティング システムのブートが完了しない場合、CIMC はシステムをリセットし、エラーがロギングされます。 次のいずれかになります。 • [Disabled]：サーバで起動時にかかる時間を追跡するためにウォッチドッグ タイマーを使用しません • [Enabled]：サーバで起動時にかかる時間をウォッチドッグ タイマーで追跡します。 **set OSBootWatchdogTimerTimeout** コマンドで指定された時間内にサーバがブートしなかった場合、CIMC によってエラーがログに記録され、**set OSBootWatchdogTimerPolicy** コマンドで指定されたアクションが実行されます。
[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、システムが実行するアクション。 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 タイマーが切れた場合、サーバの電源の状態を変更しません。 • [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、サーバの電源がオフになります。 • [Reset]：OS のブート中にウォッチドッグ タイマーが切れた場合、サーバがリセットされます。 （注） このオプションは、OS のブート ウォッチドッグ タイマーをイネーブルにする場合だけ適用されます。
set ResumeOnACPowerLoss	

第 4 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，59 ページ
- CPU のプロパティの表示，60 ページ
- メモリのプロパティの表示，60 ページ
- 電源のプロパティの表示，62 ページ
- ストレージのプロパティの表示，62 ページ
- PCI アダプタのプロパティの表示，66 ページ
- 電源ポリシーの統計情報の表示，67 ページ
- ハード ドライブのプレゼンスの表示，67 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
```

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
```

次に、DIMM サマリー情報を表示する例を示します。

```
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、シングル幅の 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、倍幅の 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、これは CIMC 経由で管理できません。
ステップ 3	Server /chassis # **scope storageadapter SLOT-***slot-number*	インストールされているストレージカードのコマンド 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アダプタ PCI の情報を表示します。
ステップ 9	Server /chassis/storageadapter # **show running-firmware-images** [**detail**]	ストレージカードで実行されているファームウェア情報を表示します。
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-***slot-number*	インストールされているストレージカードのコマンド 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*	指定し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-***slot-number*	インストールされているストレージ カードのコマンド 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 カードで設定されている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*	指定し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の情報を表示します。

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]**	サーバの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]	現在サーバで消費されているワット単位の電力。
[Maximum Consumption]	最後にリブートされてからサーバで消費された最大ワット数。
[Minimum Consumption]	最後にリブートされてからサーバで消費された最小ワット数。

この例では、シングル幅の 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、倍幅の 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
```

第 5 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。

- 障害の要約の表示，69 ページ
- 温度センサーの表示，70 ページ
- 電圧センサーの表示，70 ページ
- ストレージ センサーの表示，71 ページ

障害の要約の表示

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]**	個々のセンサーからの障害の要約を表示します。
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要約を表示します。
ステップ 4	Server /fault # **show pef [detail]**	プラットフォームイベント フィルタの要約を表示します。

この例では、個別のセンサーからの障害の要約を表示します。

```
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 #
```

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 センサーの情報を表示します。

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 ドライブがあるかないかを示します。
[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。

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 6 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，73 ページ
- 仮想メディアの設定，76 ページ
- Serial Over LAN の管理，77 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）
- コンピュータの USB フラッシュ ドライブ

KVM コンソールを使用して、オペレーティング システムまたはハイパーバイザをサーバにインストールし、次を実行できます。

- ブートアップ中に F2 キーを押して、BIOS セットアップ メニューにアクセスします。
- ブートアップ中に F8 キーを押して、CIMC Configuration Utility にアクセスします。
- ブートアップ中に 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 リダイレクト
- フロー制御なし

- SoL に設定されたのと同じボー レート
- VT 100 ターミナル タイプ
- レガシー OS のリダイレクトのディセーブル化

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

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

Serial over LAN の設定

はじめる前に

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 7 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，81 ページ
- Active Directory，82 ページ
- ユーザ セッションの表示，86 ページ
- ユーザ セッションの終了，86 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。

CIMC で Active Directory をイネーブルにすると、ローカル ユーザ データベースで見つからなかったユーザ アカウントのユーザ認証とロール許可が、Active Directory により行われます。

サーバでの Active Directory の設定で暗号化をイネーブルにすることで、サーバに Active Directory への送信データを暗号化するよう要求できます。

Active Directory サーバの設定

CIMC を設定して、Active Directory をユーザの認証と認可に使用できます。 Active Directory を使用するには、CIMC のユーザ ロールとロケールを保持する属性を使用してユーザを設定します。CIMC のユーザ ロールとロケールにマップされた既存の LDAP 属性を使用できます。または、Active Directory スキーマを変更して、属性 ID 1.3.6.1.4.1.9.287247.1 を持つ CiscoAVPair 属性のような新規のカスタム属性を追加できます。 Active Directory スキーマの変更の詳細については、http://technet.microsoft.com/en-us/library/bb727064.aspx を参照してください。

Active Directory サーバで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
一般名	CiscoAVPair
LDAP 表示名	CiscoAVPair
一意の X500 オブジェクト ID	1.3.6.1.4.1.9.287247.1
説明	CiscoAVPair
構文	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

ローカル ユーザの認証と許可に Active Directory（AD）サーバを使用するには、CIMC で Active Directory 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 コンフィギュレーションに対して 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 データベースにないユーザ アカウントに対して、ユーザ認証とロール許可が AD によって実行されます。
ステップ 3	Server /ldap # **set timeout** *seconds*	LDAP 検索操作がタイムアウトになるまで 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 に送信されるすべての情報を暗号化します。

	コマンドまたはアクション	目的
ステップ 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。
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。
[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て、関連付けられているユーザセッションを強制的に終了できる場合は、このカラムに [Terminate] と表示されます。 それ以外の場合は、N/A と表示されます。 （注） このタブから現在のセッションを終了することはできません。

次に、現在のユーザ セッションに関する情報を表示する例を示します。

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

Server /user #
```

ユーザ セッションの終了

はじめる前に

ユーザセッションを終了するには、admin権限を持つユーザとしてログインする必要があります。

手順

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

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

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

Server /user-session #
```

第 8 章

ネットワーク関連の設定

この章は、次の内容で構成されています。

- CIMC NIC の設定，89 ページ
- 共通プロパティの設定，92 ページ
- IPv4 の設定，92 ページ
- サーバ VLAN の設定，94 ページ
- ネットワーク セキュリティの設定，95 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、オンボード LAN（LOM）イーサネット ホスト ポート上の LAN、およびルータの PCIe インターフェイスと MGF インターフェイスを介して利用できます。

（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 モードおよび NIC 冗長化を設定するには、次の手順を使用します。

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 LAN On Motherboard（LOM; マザーボードのオンボード LAN）イーサネット ホスト ポートを使用します。 （注） Shared LOM を選択した場合は、すべてのホスト ポートが同じサブネットに属することを確認してください。
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 スイッチを介して 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、GE2、および GE3 の各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 インターフェイスを含むすべてのインターフェイス オプションは、倍幅 E シリーズ サーバ に対してのみ適用できます。
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 9 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，97 ページ
- SSH の設定，98 ページ
- IPMI の設定，99 ページ
- SNMP の設定，101 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。
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。

	コマンドまたはアクション	目的
		60 ～ 10,800 の範囲の整数を入力します。 デフォルトは 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。
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。

	コマンドまたはアクション	目的
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 #
```

IPMI の設定

IPMI Over LAN

Intelligent Platform Management Interface（IPMI）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 プロセッサとインターフェイスを取るためのプロトコルを定義します。 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に指示できます。

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

次の作業を実行するには、admin 権限でログインする必要があります。

手順

	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**}	このサーバの IPMI セッションで指定できる最も高い特権レベルを指定します。 次のステータスがあります。 • **readonly**：IPMI ユーザは情報を表示できますが、変更はできません このオプションを選択すると、「Administrator」、「Operator」、または「User」ユーザ ロールを持つ IPMI ユーザは、他の IPMI 特権に関係なく、読み取り専用 IPMI セッションだけを作成できます。 • **user**：IPMI ユーザは一部の機能を実行できますが、管理タスクは実行できません。 このオプションを選択すると、「Administrator」または「Operator」ユーザ ロールを持つ IPMI ユーザは、このサーバ上でユーザ セッションと読み取り専用セッションを作成できます。 • **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すると、「Administrator」ユーザ ロールを持つ IPMI ユーザは、このサーバ上で admin、ユーザ、および読み取り専用セッションを作成できます。
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、SNMP トラップによって障害とアラートに関する情報を送信するために、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 コマンドが受け取られる前に、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 ホストに送信するすべてのトラップ メッセージに含めるデフォルトの 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責任者を指定します。 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, （102 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

- 次の作業を実行するには、admin 権限でログインする必要があります。
- トラップ設定を指定するには、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 # **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**}	トラップ メッセージの必要な 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 SNMP トラップの設定値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

次の作業を実行するには、admin 権限でログインする必要があります。

手順

	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は、トラップが設定されて、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 #
```

第 10 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，105 ページ
- 証明書署名要求の生成，106 ページ
- 自己署名証明書の作成，107 ページ
- サーバ証明書のアップロード，109 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） アップロードされる証明書は、CIMC によって生成された CSR から作成される必要があります。 この方法で作成されていない証明書はアップロードしないでください。

証明書署名要求の生成

はじめる前に

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

手順

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

証明書署名要求に関して、次の情報の入力を求めるプロンプトが表示されます。

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

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

次に、証明書署名要求を生成する例を示します。

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

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


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

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

次の作業

次のいずれかの作業を実行します。

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

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

自己署名証明書の作成

パブリック認証局（CA）を使用してサーバ証明書の生成と署名を行う代わりに、独自の CA を運用して独自の証明書に署名することができます。 このセクションでは、Linux で実行されている OpenSSL 証明書サーバを使用して CA を作成するコマンドおよびサーバ証明書を生成するコマンドについて説明します。 OpenSSL の詳細については、http://www.openssl.org を参照してください。

（注） これらのコマンドは、CIMC CLI ではなく、OpenSSL パッケージを使用している Linux サーバで入力します。

はじめる前に

組織内のサーバで、証明書サーバのソフトウェア パッケージを取得してインストールします。

手順

	コマンドまたはアクション	目的
ステップ 1	**openssl genrsa -out** *CA_keyfilename keysize* 例： `# openssl genrsa -out ca.key 1024`	このコマンドは、CA で使用される RSA 秘密キーを生成します。 （注） ユーザ入力なしで CA がキーにアクセスできるように、このコマンドに -des3 オプションは使用しないでください。 指定されたファイル名には、指定されたサイズの RSA キーが含まれています。
ステップ 2	**openssl req -new -x509 -days** *numdays* **-key** *CA_keyfilename* **-out** *CA_certfilename* 例： `# openssl req -new -x509 -days 365 -key ca.key -out ca.crt`	このコマンドは、指定されたキーを使用して、CA の自己署名証明書を新規に作成します。 証明書は指定された期間有効になります。 このコマンドは、ユーザに証明書の追加情報を求めるプロンプトを表示します。 証明書サーバは、アクティブな CA です。
ステップ 3	**echo "nsCertType = server" > openssl.conf** 例： `# echo "nsCertType = server" > openssl.conf`	このコマンドは、証明書がサーバ限定の証明書であることを指定する行を OpenSSL コンフィギュレーション ファイルに追加します。 この指定により、認証されたクライアントがサーバになりすます man-in-the-middle 攻撃を防御できます。 OpenSSL コンフィギュレーション ファイル openssl.conf には、"nsCertType = server" という文が含まれています。
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 11 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，111 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，111 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，112 ページ
- プラットフォーム イベント フィルタの設定，113 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。

	コマンドまたはアクション	目的
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。

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
```

プラットフォーム イベント フィルタの設定

```
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。 • **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。

プラットフォーム イベント フィルタの設定

	コマンドまたはアクション	目的
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

第 12 章

CIMC ファームウェア管理

この章は、次の内容で構成されています。

- CIMC ファームウェアの概要，115 ページ
- シスコからのソフトウェアの取得，116 ページ
- TFTP サーバからの CIMC ファームウェアのインストール，118 ページ
- インストールされている CIMC ファームウェアのアクティブ化，119 ページ
- CIMC 情報の表示，119 ページ

CIMC ファームウェアの概要

E シリーズ サーバは、cisco.com からダウンロードしたファームウェアを使用します。このファームウェアは、シスコによって認証され、E シリーズ サーバ でアップグレードされます。

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

注意 この .zip ファイルを使用してサーバの更新を行わないでください。

再イメージ化には .bin ファイルを使用します。 この .zip ファイルから適切な .bin アップグレード ファイルを展開する必要があります。 この .bin ファイルは、TFTP サーバまたはローカル マシンに展開できます。 TFTP サーバを使用して更新できます。

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

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

インストール

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

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

アクティブ化

この段階では、CIMC は非アクティブのファームウェア バージョンをアクティブとして設定し、サーバを再起動します。 サーバを再起動すると、非アクティブ スロットはアクティブ スロットになり、アクティブ スロットは非アクティブ スロットになります。 新規のアクティブ スロット内のファームウェアが、実行中のバージョンとなります。

シスコからのソフトウェアの取得

ドライバ、BIOS、CIMC 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/ に移動します。

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

ステップ 3 上部のメニュー バーで、[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 ダウンロード（中央）のペインで、[All Downloads] をクリックします（右下隅に配置）。
[Download Software] ページが表示されます。

ステップ 5 左側のペインで、[Products] をクリックします。

ステップ 6 中央のペインの [Unified Computing and Servers] をクリックします。

ステップ 7 右側のペインで、[Cisco UCS E-Series Software] をクリックします。

ステップ 8 右側のペインで、ソフトウェアをダウンロードするサーバ モデルの名前をクリックします。
[Download Software] ページが表示され、次のような、ダウンロードできるソフトウェア カテゴリのリストが表示されます。

- [Unified Computing System (UCSE) Server Drivers]：次のドライバが含まれています。
  - Windows 2008 R2 用のオンボード ネットワーク ドライバ
  - Windows 2008 R2 および Linux 用の 10G PCIe 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
- [Unified Computing System (UCSE) Server Firmware]：次の BIOS および CIMC ファームウェア イメージが含まれています。
  - 倍幅 BIOS
  - シングル幅 BIOS
  - BMC/CIMC イメージ
- [Unified Computing System (UCSE) Utilites]：次の診断イメージが含まれています。
  - オンボード診断イメージ

ステップ 9 該当するソフトウェア カテゴリの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た [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、次の手順を実行します。

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た [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) すべてのイメージをダウンロードするには、右下隅にある [Download All] 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 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。

- ローカル ドライブにソフトウェア イメージ ファイルを保存します。
- TFTP サーバからソフトウェア イメージを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の読み取り権限を持つ必要があります。

次の作業

ソフトウェア イメージをインストールします。

TFTP サーバからの CIMC ファームウェアのインストール

はじめる前に

シスコから CIMC ファームウェアを取得し、そのファイルをローカル TFTP サーバに保存します。「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アップデートを開始すると、どちらのアップデートも失敗します。

手順

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

インストールされているCIMCファームウェアのアクティブ化

はじめる前に

CIMC ファームウェアをサーバにインストールします。

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

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
```

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 に関する情報を表示する例を示します。

```
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
```

第 13 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，121 ページ
- システム イベント ログ，124 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
```

リモート サーバへの CIMC ログの送信

CIMC ログ エントリを受信するように 1 台または 2 台のリモート syslog サーバのプロファイルを設定できます。

はじめる前に

- リモート syslog サーバは、リモート ホストからログを受信するように設定されている必要があります。

- リモート syslog サーバは、認証関連のログを含む、すべてのタイプのログを受信するように設定されている必要があります。
- リモート syslog サーバのファイアウォールは、syslog メッセージが syslog サーバに到達するように設定されている必要があります。

手順

	コマンドまたはアクション	目的
ステップ 1	Server# **scope 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 #
```

システム イベント ログ

システム イベント ログの表示

手順

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

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 14 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。

- テクニカル サポート データのエクスポート，127 ページ
- CIMC の再起動，128 ページ
- CIMC の出荷時デフォルトへのリセット，129 ページ
- CIMC コンフィギュレーションのエクスポートおよびインポート，130 ページ

テクニカル サポート データのエクスポート

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

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 tftp-ip** *ip-address*	サポート データ ファイルを保存する必要のある TFTP サーバの IP アドレスを指定します。
ステップ 4	Server /cimc/tech-support # **set path** *path/filename*	サーバでサポート データを保存する必要のあるファイルの名前を指定します。 この名前を入力するときは、ファイルの相対パスを、TFTP ツリーの最上位から目的の場所まで含めてください。

	コマンドまたはアクション	目的
ステップ 5	Server /cimc/tech-support # **commit**	トランザクションをシステムの設定にコミットします。
ステップ 6	Server /cimc/tech-support # **start**	TFTP サーバへのサポート データ ファイルの転送を開始します。
ステップ 7	Server /cimc/tech-support # **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 8	Server /cimc/tech-support # **cancel**	（任意）TFTP 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 tftp-ip 10.20.30.41
Server /cimc/tech-support *# set path /user/user1/supportfile
Server /cimc/tech-support *# commit
Server /cimc/tech-support # start
Server /cimc/tech-support # show detail
```

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コンフィギュレーションのエクスポートおよびインポート

CIMC コンフィギュレーションのエクスポートおよびインポート

CIMC コンフィギュレーション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、ネットワーク上のロケーションに結果の CIMC コンフィギュレーション ファイルをエクスポートします。 エクスポート操作では、管理プレーンの情報だけが保存されます。サーバのデータはバックアップされません。ユーザアカウントやサーバ証明書などの機密性の高い設定情報はエクスポートされません。

エクスポートされた CIMC コンフィギュレーション ファイルは、同じシステムに復元できます。また、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、または設定の互換性があれば、別の CIMC システムにインポートすることもできます。 設定テンプレートとして別のシステムにコンフィギュレーション ファイルをインポートした場合は、IP アドレスやホスト名など、システム固有の設定を修正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 コンフィギュレーション ファイルは、構造と要素が CIMC コマンド モードに対応する XML テキスト ファイルです。

エクスポートまたはインポート操作を実行する場合は、次の注意事項に従ってください。

- エクスポートまたはインポートは、システムが起動されて動作している間に実行できます。エクスポート操作はサーバまたはネットワーク トラフィックに影響しませんが、インポート操作によって IP アドレスの変更など一部の修正が発生すると、トラフィックの中断またはサーバのリブートが発生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 コンフィギュレーションのエクスポート

（注） セキュリティ上の理由から、この操作ではユーザアカウントおよびサーバ証明書はエクスポートされません。

はじめる前に

- バックアップ TFTP サーバの IP アドレスを取得します。
- コンフィギュレーション ファイルをインポートする場合に SNMP 設定情報を復元するオプションを使用する場合は、コンフィギュレーションファイルを作成する前に、SNMP がこのサーバでイネーブルであることを確認します。 設定のエクスポート時に SNMP がディセーブルの場合、CIMC では、ファイルをインポートしたときに、SNMP 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 アドレスの TFTP サーバで指定され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 キーを押します。

次に、CIMC コンフィギュレーションをバック 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 コンフィギュレーションのインポート

はじめる前に

コンフィギュレーション ファイルをインポートするときに、SNMP 設定情報を復元する場合は、インポートを行う前に SNMP がこのサーバでディセーブルになっていることを確認します。インポートを実行するときに SNMP がイネーブルの場合、CIMC では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現在の値を上書きしません。

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 アドレスの TFTP サーバで指定されたパスとファイル名で、コンフィギュレーション ファイルは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 キーを押します。

次に、CIMC コンフィギュレーションをインポートする例を示します。

```
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 15 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，133 ページ
- ホストへの診断イメージのマッピング，134 ページ
- 診断テストの実行，135 ページ

診断テストの概要

診断は、サーバで実行されているオペレーティング システムやアプリケーションから独立して E シリーズ サーバで動作するスタンドアロン ユーティリティです。 E シリーズ サーバで問題が発生した場合、予備的なチェックを実行し、問題を分離するために、診断テストを使用できます。診断テストは、サーバ CPU、メモリ、およびブロック デバイス上で実行できます。 ブロック デバイスにはハード ドライブ、USB ドライブ、および SD カードが含まれます。

診断テストが成功すれば、サーバCPU、メモリ、またはブロック デバイスに問題はありません。問題は他のハードウェア コンポーネントまたはソフトウェアの設定にあると考えられます。問題を特定するために、http://www.cisco.com/cisco/web/support/index.html で、Cisco Technical Assistance Center（TAC）へのサービス要求を開始してください。

診断テストに失敗したら、Cisco TAC へのサービス要求を開始して、さらにアドバイスを得てください。

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障害が発生すると、ディスクの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する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 診断イメージは購入時にEシリーズサーバにプリインストールされています。 指定したFTP、FTPS、HTTP、またはHTTPSサーバからCIMC内部リポジトリに最新の診断イメージをダウンロードすることもできます。

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

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。
- 診断イメージは購入時にEシリーズサーバにプリインストールされています。 指定したFTP、FTPS、HTTP、またはHTTPSサーバからCIMC内部リポジトリに最新の診断イメージを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の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.diagである必要があります。 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に従って診断テストを実行します。

はじめる前に

- データをバックアップします。すべてのテストは破壊的ではありませんが、テストの実行中に電源または装置に障害が発生すると、ディスク データが損傷を受け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することを強くお勧めします。

- 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 ドライブにあるすべてのファイル パッケージが表示されます。 デバイスの名前は fs0 から始まり、fs0、fs1、fs2 のように続きます。 （注） 仮想メディア ドライブ名の後にコロンを追加してください。 たとえば、dir fs1: のようにします。
ステップ 2	Shell > *virtual-media-drive-name*:	診断ファイルが含まれている仮想メディア ドライブを開始します。
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のパッケージ 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。 確認のプロンプトが表示されたら、y で応答します。
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、テストの進捗およびステータスを表示します。 診断テストは、サーバ CPU、メモリ、およびブロック デバイスに対して実行されます。 ブロック デバイスにはハード ドライブ、USB ドライブ、および SD カードが含まれます。 サーバに対して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。ここで、*test-name* は次のいずれかにすることができます。 • cpux64：CPU 診断テスト。 • diskx64：ブロック デバイス診断テスト。 ブロック デバイスにはハード ドライブ、USB ドライブ、および SD カードが含まれます。 • memoryx64：メモリ診断テスト。 （注） 診断テストの実行には、約 10 分間かかる場合があります。
ステップ 6	（任意）Server: SRV > **results**	Passed または Failed のテスト ステータスとともに、診断テストの要約が表示されます。

	コマンドまたはアクション	目的
		（注） 要約レポートには、失敗したテストと成功したテストの数が示されます。 どのテストが失敗または成功したかに関する情報は提供されません。どのテストが失敗または成功したかを判別するには、run all コマンドの出力を参照してください。
ステップ 7	（任意）Server: SRV > **show**	サーバで管理されていたグローバルパラメータおよび診断テスト モジュールのリストが表示されます。
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 へのサービス要求を開始します。	診断テストが成功すれば、サーバCPU、メモリ、またはブロック デバイスに問題はありません。 問題は他のハードウェア コンポーネントまたはソフトウェアの設定にあると考えられます。 Cisco TAC へのサービス要求を開始して、問題を特定します。 診断テストに失敗したら、Cisco TAC へのサービス要求を開始して、さらにアドバイスを得てください。

次に、すべての診断テストを実行する例を示します。

```
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 82, 83, 84
  CIMC での設定 84

B

BIOS 42, 44, 45, 116
  CMOS 44
    クリア 44
  シスコからのファームウェアの取得 116
  パスワード 45
    クリア 45
  ファームウェア 42
    TFTP サーバからのインストール 42
BIOS CMOS 44
  クリア 44
BIOS ステータス 41
  表示 41
BIOS 設定 43, 44, 45, 46
  概要 46
  高度 43
  サーバ管理 44
  デフォルトの復元 45
BIOS パスワード 45
  クリア 45
BIOS ファームウェア 42
  TFTP サーバからのインストール 42

C

CIMC 115, 116, 118, 119, 121, 122, 129
  シスコからのファームウェアの取得 116
  出荷時デフォルト値へのリセット 129
  ファームウェア 115, 118, 119
    TFTP サーバからのインストール 118
CIMC (続き)
  ファームウェア (続き)
    アクティブ化 119
    概要 115
  ファームウェアの詳細 119
  ログのクリア 122
  ログの送信 122
  ログの表示 121
CIMC CLI 4
CIMC NIC 89
CIMC の概要 3
CIMC ファームウェア 119
  アクティブ化 119
CIMC ファームウェアの詳細 119
  表示 119
CPU のプロパティ 60

E

E シリーズ サーバ 1
  概要 1

H

HTTP のプロパティ 97

I

IPMI over LAN 99
  説明 99
IPMI over LAN のプロパティ 99
IPv4 のプロパティ 92
IP ブロッキング 95

K

KVM 74, 75
　イネーブル化 74, 75
　設定 74
　ディセーブル化 75
KVM コンソール 11, 73
KVM のイネーブル化 74, 75
KVM のディセーブル化 75

L

LDAP。参照先： Active Directory

N

NIC のプロパティ 90

O

OS のインストール 11, 13
　PXE 13
　方法 11

P

PCI アダプタ 66
　プロパティの表示 66
PXE インストール 12

R

RAID 27, 38
　削除 38
　設定 27
RAID オプション 23

S

Serial over LAN 77, 78, 79
　起動 79
　設定 78
SNMP 101, 102, 103
　テスト メッセージの送信 103
SNMP *(続き)*
　トラップ設定の指定 102
　プロパティの設定 101
SSH のプロパティ 98
syslog 122
　CIMC ログの送信 122

V

VLAN のプロパティ 94
VMware 18
　ソフトウェアの取得 18

Y

YAML 8

あ

アダプタ 66
　PCI 66

い

イベント 111, 112
　プラットフォーム 111, 112
　　アラートのイネーブル化 111
　　アラートのディセーブル化 112
イベント フィルタ、プラットフォーム 111, 113
　概要 111
　設定 113
イベント ログ、システム 124, 125
　クリア 125
　表示 124
インポート 132
　CIMC コンフィギュレーション 132

え

エクスポート 130, 131
　CIMC コンフィギュレーション 130, 131

お

温度センサー 70

か

仮想 KVM 74, 75
仮想ドライブ 32, 34, 36
　オプションの再構築 34
　再構築 36
　整合性検査の実行 32
仮想メディア 76
仮想メディアの暗号化 76

き

共通プロパティ 92

こ

コミュニケーション サービスのプロパティ 97, 98, 99
　HTTP のプロパティ 97
　IPMI over LAN のプロパティ 99
　SSH のプロパティ 98
コンフィギュレーション 130, 131, 132
　インポート 132
　エクスポート 130
　バックアップ 131

さ

サーバ管理 19, 20, 21, 22, 23
　サーバ電源の再投入 23
　サーバのシャットダウン 21
　サーバの電源オフ 22
　サーバの電源投入 21
　サーバのリセット 20
　ブート順の設定 19
サーバ証明書のアップロード 109
サーバ ソフトウェア 2
サーバ電源の再投入 23
サーバのシャットダウン 21
サーバの電源オフ 22
サーバの電源投入 21
サーバのプロパティ 59
サーバのリセット 20
削除 17

し

自己署名証明書 107
システム イベント ログ 124, 125
　クリア 125
　表示 124
自動再構築、イネーブル化 32
障害の要約 69
　表示 69
証明書管理 109
　証明書のアップロード 109
診断 135
　テスト、実行 135
診断イメージ 134

す

ストレージ センサー 71
　表示 71
ストレージのプロパティ 62, 64, 65
　アダプタのプロパティの表示 62
　仮想ドライブのプロパティの表示 65
　物理ドライブのプロパティの表示 64

せ

センサー 70
　温度 70
　電圧 70

そ

ソフトウェア 18
　VMware の取得 18

て

ディスク ドライブのブート可能化 30
　CIMC CLI の使用 30

テクニカル サポート データ、エクスポート 127
電圧センサー 70
電源のプロパティ 62
電源ポリシーの統計情報 67
　表示 67

ね

ネットワーク セキュリティ 95
ネットワーク プロパティ 90, 92, 94
　IPv4 のプロパティ 92
　NIC のプロパティ 90
　VLAN のプロパティ 94
　共通プロパティ 92

は

ハード ドライブのプレゼンス 67
バックアップ 130, 131
　CIMC コンフィギュレーション 130, 131

ふ

ファームウェア 115, 116, 118
　TFTP サーバからのインストール 118
　概要 115
　シスコからの取得 116
ブート順、設定 19
物理ドライブ 40
　再構築 40
物理ドライブの状態 39
　変更 39
プラットフォーム イベント 111, 112
　アラートのイネーブル化 111
　アラートのディセーブル化 112
プラットフォーム イベント フィルタ 111, 113
　概要 111
　設定 113
フロッピー ディスクのエミュレーション 76

ほ

ホストのイメージ 14, 16, 17
ホストのイメージ マッピング 13
ホストへのマッピング 134

ま

マッピング 14
マッピング解除 16

め

メモリのプロパティ 60

ゆ

ユーザ管理 81, 84, 86
　Active Directory 84
　終了、ユーザ セッション 86
　ユーザ セッションの表示 86
　ローカル ユーザ 81
ユーザ セッション 86
　終了 86
　表示 86

り

リモート プレゼンス 74, 75, 76, 78, 79
　Serial Over LAN の起動 79
　Serial over LAN の設定 78
　仮想 KVM 74, 75
　仮想メディア 76

ろ

ローカル ユーザ 81