



Cisco UCSE シリーズサーバと **Cisco UCSE** シリーズネットワーク コンピューターエンジンの統合管理コントローラ リリース **3.1.1 GUI** コンフィギュレーションガイド

初版：2016年07月06日

最終更新：2016年07月06日

シスコシステムズ合同会社

〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー

<http://www.cisco.com/jp>

お問い合わせ先：シスコ コンタクトセンター

0120-092-255（フリーコール、携帯・PHS含む）

電話受付時間：平日 10:00～12:00、13:00～17:00

<http://www.cisco.com/jp/go/contactcenter/>

【注意】 シスコ製品をご使用になる前に、安全上の注意（www.cisco.com/jp/go/safety_warning/）をご確認ください。本書は、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。また、契約等の記述については、弊社販売パートナー、または、弊社担当者にご確認ください。

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

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

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

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

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

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

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

© 2016 Cisco Systems, Inc. All rights reserved.



目次

はじめに ix

新機能および変更された機能に関する情報 ix

対象読者 x

マニュアルの構成 x

表記法 xii

関連資料 xiv

マニュアルの入手方法およびテクニカル サポート xiv

概要 1

Cisco UCS E シリーズ サーバおよび Cisco UCS E シリーズ ネットワーク コンピュート エンジンの概要 1

サーバ ソフトウェア 2

CIMC の概要 3

CIMC GUI 4

CIMC GUI へのログイン 4

CIMC ホーム ページ 5

[Navigation] ペインと [Work] ペイン 6

ツールバー 7

CIMC オンライン ヘルプ 8

CIMC GUI からのログアウト 8

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 9

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 9

KVM コンソール 10

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 11

PXE インストール サーバ 13

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
カスタマイズされた VMware vSphere Hypervisor イメージのダウンロード	14
ホスト イメージ マッピング	15
ホスト イメージのマッピング	15
ホスト イメージのマッピング解除	17
ホスト イメージの削除	18
サーバの管理	19
全体のサーバ ステータスの表示	19
CIMC GUI を使用したサーバのブート順の設定	21
BIOS セットアップ メニューを使用したブート順の設定	24
サーバのリセット	25
サーバのシャットダウン	25
Cisco IOS CLI 設定変更のロックまたはロック解除	26
サーバの電源管理	27
サーバの電源投入	27
サーバの電源オフ	27
サーバ電源の再投入	28
電力復元ポリシーの設定	29
サーバの前面パネルにある電源ボタンのロックまたはロック解除	30
サーバの前面パネルにあるリセット ボタンのロックまたはロック解除	31
BIOS の設定	32
バックアップ BIOS のアクティブ化	32
BIOS の詳細設定	32
サーバ管理 BIOS の設定	34
BIOS CMOS のクリア	36
BIOS パスワードのクリア	36
サーバ BIOS 設定	37
トラステッドプラットフォーム モジュールの設定	49
RAID を使用したストレージの管理	51
RAID オプション	52
RAID の設定	55

RAID 設定の変更	58
RAID 設定の削除	59
物理ドライブの状態の変更	60
物理ドライブの再構築	61
物理ドライブの内容のクリア	62
ストレージコントローラ上での自動再構築のイネーブル化	62
仮想ドライブの削除	63
仮想ドライブの整合性検査の実行	64
仮想ドライブの再構築のオプション	64
仮想ドライブの再構築	67
ブート可能な仮想ドライブまたは物理ドライブの作成	68
2 TB を超える RAID ボリュームをサポートするための W2K12 のインストール	70
2 TB を超える RAID ボリュームをサポートするための、レガシー BIOS を使用した W2K12 のインストール	71
2 TB を超える RAID ボリュームをサポートするための、UEFI を使用した W2K12 のインストール	88
サーバのプロパティの表示	103
サーバのプロパティの表示	103
CIMC 情報の表示	104
ルータ情報の表示	105
CPU のプロパティの表示	105
メモリのプロパティの表示	106
電源のプロパティの表示	109
ストレージのプロパティの表示	109
PCI アダプタのプロパティの表示	111
電力統計情報の表示	112
インターフェイスの MAC アドレスの表示	112
CIMC ネットワーク接続の状態の表示	113
サーバのセンサーの表示	115
温度センサーの表示	115
電圧センサーの表示	116
LED センサーの表示	117

ストレージセンサーの表示	118
リモート プレゼンスの管理	121
仮想 KVM の管理	121
KVM コンソール	121
仮想 KVM の設定	122
仮想 KVM のイネーブル化	123
仮想 KVM のディセーブル化	124
仮想メディアの設定	124
CIMC マップされた vMedia ボリュームの作成	125
CIMC マップされた vMedia ボリュームのプロパティの表示	128
CIMC マップされた vMedia ボリュームの削除	129
Serial over LAN の設定	129
ユーザアカウントの管理	131
ローカルユーザの設定	131
LDAP サーバ (Active Directory)	132
LDAP サーバの設定	133
CIMC での LDAP 設定およびグループ許可の設定	134
ユーザセッションの表示	139
ネットワーク関連の設定	141
CIMC NIC の設定	141
CIMC NIC	141
CIMC NIC の設定	142
共通プロパティの設定	144
IPv4 の設定	145
VLAN への接続	146
ネットワークセキュリティの設定	146
ネットワークセキュリティ	146
ネットワークセキュリティの設定	147
ネットワーク解析機能の有効化	148
NTP 設定の構成	148
NTP 設定	148
NTP 設定の構成	148

コミュニケーションサービスの設定	151
HTTP の設定	151
SSH の設定	152
XML API の設定	153
CIMC の XML API	153
XML API のイネーブル化	153
IPMI の設定	154
IPMI over LAN	154
IPMI over LAN の設定	154
SNMP の設定	156
SNMP	156
SNMP プロパティの設定	156
SNMP トラップ設定の指定	157
SNMP テスト トラップ メッセージの送信	159
SNMP ユーザの設定	159
SNMP ユーザの管理	161
証明書管理	163
サーバ証明書の管理	163
証明書署名要求の生成	164
自己署名証明書の作成	165
サーバ証明書のアップロード	167
プラットフォーム イベント フィルタの設定	169
プラットフォーム イベント フィルタ	169
プラットフォーム イベント アラートのイネーブル化	169
プラットフォーム イベント アラートのディセーブル化	170
プラットフォーム イベント フィルタの設定	170
プラットフォーム イベント トラップの解釈	171
ファームウェア管理	175
ファームウェアの概要	175
ファームウェアのアップグレードのオプション	176
シスコからのソフトウェアの取得	177
リモートサーバからの CIMC ファームウェアのインストール	178
ブラウザ経由の CIMC ファームウェアのインストール	180

インストールした CIMC ファームウェアのアクティブ化	181
ブラウザ経由の BIOS ファームウェアのインストール	182
TFTP サーバからの BIOS ファームウェアのインストール	183
障害およびログの表示	185
障害	185
障害サマリーの表示	185
障害履歴の表示	187
システム イベント ログ	188
システム イベント ログの表示	188
システム イベント ログのクリア	189
Cisco IMC Log	189
CIMC ログの表示	189
CIMC ログのクリア	190
CIMC ログしきい値の設定	191
リモート サーバへの CIMC ログの送信	192
サーバユーティリティ	195
テクニカル サポート データのエクスポート	195
リモート サーバへのテクニカル サポート データのエクスポート	195
ローカル ファイルへのテクニカル サポート データのダウンロード	196
CIMC の再起動	197
CIMC の出荷時デフォルトへのリセット	198
CIMC 設定のエクスポートとインポート	199
CIMC 設定のエクスポートとインポート	199
CIMC 設定のエクスポート	199
CIMC 設定のインポート	201
ログイン バナー ファイルの内容の変更	202
診断テスト	205
診断テストの概要	205
ホストへの診断イメージのマッピング	206
診断テストの実行 : E シリーズ サーバおよび SME シリーズ NCE	208
診断テストの実行 : EHWIC E シリーズ NCE および NIM E シリーズ NCE	211



はじめに

この前書きは、次の項で構成されています。

- [新機能および変更された機能に関する情報](#), ix ページ
- [対象読者](#), x ページ
- [マニュアルの構成](#), x ページ
- [表記法](#), xii ページ
- [関連資料](#), xiv ページ
- [マニュアルの入手方法およびテクニカルサポート](#), xiv ページ

新機能および変更された機能に関する情報

次の表は、この最新リリースに関するガイドでの主な変更点の概要を示したものです。

表 1: *Cisco Integrated Management Controller Software* リリース 3.1.1 の新機能と重要な動作の変更

機能	説明	参照先
UCS-E160S-M3/K9 サーバのサポート	Cisco ISR 4000 シリーズに UCS-E160S-M3/K9 の設置に対するサポートが追加されました。	概要 , (1 ページ)

表 2: *Cisco Integrated Management Controller Software* リリース 3.0.1 の新機能と重要な動作の変更

機能	説明	参照先
NIM E シリーズ ネットワーク コンピュート エンジン サポート	NIM E シリーズ ネットワーク コンピュート エンジン (NIM E シリーズ NCE) のサポート。	概要 , (1 ページ)

機能	説明	参照先
障害およびログ	<p>[Navigation] ペインの [Server] タブにある [Fault Sensors] が [Faults and Logs] に変更されました。</p> <p>[Faults and Logs] タブの下に、次の新しいタブが追加されました。[Fault History]、[Cisco IMC Log]、[Logging Controls]。</p> <p>(注) 以前のリリースでは、[CIMC Log] (現 [Cisco IMC Log]) タブと [Logging Controls] タブは、[Admin] タブの下にありました。</p>	障害およびログの表示, (185 ページ)
ネットワーク解析モジュール (NAM) および Network Time Protocol (NTP) の設定	NAM 機能と NTP サービスを有効にするためのサポートが追加されました。	ネットワーク関連の設定, (141 ページ)
ログイン バナー ファイル	CIMC ログインページにバナーが追加されました。バナー ファイルの内容は、CIMC GUI の [Utilities] ページで変更できます。	サーバユーティリティ, (195 ページ)

対象読者

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

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

マニュアルの構成

このマニュアルの構成は、次のとおりです。

章	タイトル	説明
第 1 章	概要	Cisco UCS E-Series Servers、Cisco UCS E シリーズ ネットワーク コンピュート エンジン、および CIMC GUI の概要を紹介しします。
第 2 章	サーバのオペレーティングシステムのインストール	サーバ上のオペレーティングシステム (OS) の設定方法を説明しします。
第 3 章	サーバの管理	サーバのブート デバイスの順序、サーバの電源、電力使用ポリシー、および BIOS の設定方法について説明しします。
第 4 章	RAID を使用したストレージの管理	RAID を設定および管理する手順について説明しします。 (注) RAID 機能は E シリーズ サーバおよび SM E シリーズ NCE に適用されます。RAID 機能は EHWIC E シリーズ NCE および NIM E シリーズ NCE には適用されません。
第 5 章	サーバのプロパティの表示	サーバの CPU、メモリ、電源、ストレージ、PCI アダプタ および LOM のプロパティの表示方法について説明しします。
第 6 章	サーバのセンサーの表示	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します。
第 7 章	リモートプレゼンスの管理	仮想 KVM、仮想メディア、および Serial over LAN 接続の設定方法を説明しします。
第 8 章	ユーザアカウントの管理	ユーザアカウントの追加または変更方法、Active Directory によるユーザ認証の設定方法、ユーザセッションの管理方法を説明しします。
第 9 章	ネットワーク関連の設定	ネットワークインターフェイス、ネットワーク設定、ネットワークセキュリティ、NAM、および NTP の設定方法を説明しします。
第 10 章	コミュニケーションサービスの設定	HTTP、SSH、IPMI、および SNMP によるサーバ管理コミュニケーションの設定方法を説明しします。
第 11 章	証明書の管理	サーバ証明書を生成、アップロード、および管理する方法を説明しします。

章	タイトル	説明
第 12 章	プラットフォーム イベントフィルタの設定	プラットフォーム イベント フィルタを設定および管理する方法を説明します。
第 13 章	ファームウェア管理	ファームウェア イメージを取得、インストール、およびアクティブにする方法を説明します。
第 14 章	障害およびログの表示	障害情報の表示方法、CIMC ログとシステム イベント ログ メッセージの表示、エクスポート、およびクリア方法を説明します。
第 15 章	サーバユーティリティ	サポート データのエクスポート方法、サーバ設定のエクスポート方法とインポート方法、サーバ設定を出荷時デフォルトにリセットする方法、管理インターフェイスのリポート方法を説明します。
第 16 章	診断テスト	診断テストの実行方法を説明します。

表記法

テキストのタイプ	説明
GUI 要素	タブの見出し、領域名、フィールドラベルなどの GUI 要素は、イタリック体 (<i>italic</i>) で示しています。 ウィンドウ、ダイアログボックス、ウィザードのタイトルのようなメインタイトルは、[Main titles] のように示しています。
ユーザ入力	表示どおりにユーザが入力するテキストやユーザが押すキーは、このフォント (例 : this font) で示しています。
マニュアルのタイトル	マニュアルのタイトルは、イタリック体 (<i>italic</i>) で示しています。
システム出力	システムが表示するターミナルセッションおよび情報は、courier フォントで示しています。
CLI コマンド	CLI コマンドのキーワードは、ボールド体 (this font) で示しています。 CLI コマンドの引数は、このフォント (例 : <i>this font</i>) で示しています。
[]	角カッコの中の要素は、省略可能です。

テキストのタイプ	説明
{x y z}	どれか1つを選択しなければならない必須キーワードは、波カッコで囲み、縦棒で区切って示しています。
[x y z]	どれか1つを選択できる省略可能なキーワードは、角カッコで囲み、縦棒で区切って示しています。
string	引用符を付けない一組の文字。 string の前後には引用符を使用しません。引用符を使用すると、その引用符も含めて string とみなされます。
<>	パスワードのように出力されない文字は、山カッコで囲んで示しています。
[]	システム プロンプトに対するデフォルトの応答は、角カッコで囲んで示しています。
!, #	コードの先頭に感嘆符 (!) またはポンド記号 (#) がある場合には、コメント行であることを示します。



(注) 「注釈」です。役立つ情報や、このマニュアル以外の参照資料などを紹介しています。



ヒント 「問題解決に役立つ情報」です。ヒントには、トラブルシューティングや操作方法ではなく、ワンポイントアドバイスと同様に知っておくと役立つ情報が記述される場合もあります。



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



ワンポイントアドバイス 「時間の節約に役立つ操作」です。ここに紹介している方法で作業を行うと、時間を短縮できます。

**警告** 安全上の重要事項

「危険」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。機器の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止対策に留意してください。各警告の最後に記載されているステートメント番号を基に、装置に付属の安全についての警告を参照してください。

これらの注意事項を保管しておいてください。

関連資料

『[Documentation Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine](#)』にはすべての製品ドキュメントへのリンクが示されています。

マニュアルの入手方法およびテクニカル サポート

マニュアルの入手方法、テクニカル サポート、その他の有用な情報について、毎月更新される『[What's New in Cisco Product Documentation](#)』を参照してください。シスコの新規および改訂版の技術マニュアルの一覧も示されています。

『*What's New in Cisco Product Documentation*』は RSS フィードとして購読できます。また、リーダー アプリケーションを使用してコンテンツがデスクトップに直接配信されるように設定することもできます。RSS フィードは無料のサービスです。シスコは現在、RSS バージョン 2.0 をサポートしています。

ドキュメントの更新通知を受け取るには、[Cisco UCS Docs on Twitter](#) をフォローしてください。



第 1 章

概要

この章は、次の項で構成されています。

- [Cisco UCS E シリーズ サーバおよび Cisco UCS E シリーズ ネットワーク コンピュート エンジンの概要, 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 GUI, 4 ページ](#)

Cisco UCS E シリーズ サーバおよび Cisco UCS E シリーズ ネットワーク コンピュート エンジンの概要

Cisco UCS E-Series Servers (E シリーズ サーバ) および Cisco UCS E シリーズ ネットワーク コンピュート エンジン (NCE) はサイズ、重量、電力の効率にすぐれたブレードサーバのファミリーで、第 2 世代の Cisco サービス統合型ルータ (Cisco ISR G2) および Cisco ISR 4000 シリーズに搭載されています。これらのサーバは、オペレーティングシステム (Microsoft Windows や Linux など) 上でベアメタルとして、あるいはハイパーバイザ (VMware vSphere Hypervisor、Microsoft Hyper-V、Citrix XenServer など) 上で仮想マシンとして導入される、ブランチオフィスアプリケーション向けの汎用コンピューティング プラットフォームを提供します。

E シリーズ サーバは、汎用コンピューティングの強力な Intel Xeon プロセッサ用に特別に作られています。また、シングル幅とダブル幅の 2 種類のフォーム ファクタがあります。シングル幅の E シリーズ サーバは単一のサービス モジュール (SM) スロットに適しており、ダブル幅の E シリーズ サーバは 2 つの SM スロットに適しています。

NCE は価格と性能の点で最適化されたモジュールで、シスコのネットワーク アプリケーションおよび他の軽量な汎用アプリケーションをホストするようにビルドされています。これらは、SM、NIM、および EHWIC の 3 つのフォーム ファクタで提供されます。SM E シリーズ NCE は 1 つの SM スロットに、NIM E シリーズ NCE は 1 つの NIM スロットに、EHWIC E シリーズ NCE は 2 つの EHWIC スロットに収納できます。



(注)

- EHWIC E シリーズ NCE は Cisco ISR G2 にのみ設置できます。
- NIM E シリーズ NCE は Cisco ISR 4000 シリーズにのみ設置できます。
- Cisco ISR 4331 には SM スロットが 1 つあります。Cisco ISR 4321 および Cisco ISR 4431 には SM スロットがありません。
- Citrix XenServer は E シリーズ サーバでのみサポートされます。
- Cisco UCS-E160S-M3/K9 サーバは、ISR 4000 シリーズでのみサポートされます。



(注)

サポートされている E シリーズ サーバおよび NCE の詳細、ルータごとにインストール可能なサーバの最大数については、『*Hardware Installation Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine*』の「Hardware Requirements」の項を参照してください。

サーバソフトウェア

E シリーズ サーバと NCE には、3 つの主要なソフトウェア システムが必要です。

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

CIMC ファームウェア

Cisco Integrated Management Controller (CIMC) は、E シリーズ サーバまたは NCE のマザーボードに組み込まれている別の管理モジュールです。専用の ARM ベースのプロセッサが (メイン サーバ CPU から独立して) CIMC ファームウェアを実行します。システムには、現行バージョンの CIMC ファームウェアが付属しています。CIMC ファームウェアは更新可能ですが、初期インストールは必要ありません。

CIMC は E シリーズ サーバおよび NCE 用の管理サービスです。Web ベースの GUI または SSH ベースの CLI を使用して、サーバにアクセスし、サーバを設定、管理、モニタできます。

BIOS ファームウェア

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

システムには、現行バージョンの BIOS ファームウェアが付属しています。BIOS ファームウェアは更新可能ですが、初期インストールは必要ありません。

オペレーティング システムまたはハイパーバイザ

メイン サーバ CPU は 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 が事前にインストールされている E シリーズ サーバまたは NCE を購入することも、独自のプラットフォームをインストールすることもできます。



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

CIMC の概要

Cisco Integrated Management Controller (CIMC) は、E シリーズ サーバおよび NCE 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



(注) RAID 機能は E シリーズ サーバおよび SM E シリーズ NCE に適用されます。RAID 機能は EHWIC E シリーズ NCE および NIM E シリーズ NCE には適用されません。

- サーバのプロパティとセンサーを表示する
- リモート プレゼンスを管理する
- ローカル ユーザ アカウントを作成して管理し、Active Directory によるリモート ユーザの認証をイネーブルにする
- NIC プロパティ、IPv4、VLAN、ネットワーク セキュリティなど、ネットワーク関連の設定を行う
- HTTP、SSH、IPMI over LAN、SNMP などのコミュニケーション サービスを設定する
- 証明書を管理する
- プラットフォーム イベント フィルタを設定する

- CIMC ファームウェアを更新する
- BIOS ファームウェアを更新する
- 内部リポジトリからホスト イメージをインストールする
- 障害、アラーム、およびサーバのステータスをモニタする
- サーバ障害の発生時にテクニカル サポート データを収集する

ほとんどすべてのタスクは、GUI インターフェイスと CLI インターフェイスのいずれでも実行できます。また、一方のインターフェイスで実行されたタスクの結果は、もう一方のインターフェイスにも表示されます。ただし、以下のことは実行できません。

- CIMC GUI を使用して CIMC CLI を呼び出すことはできない
- CIMC CLI で呼び出したコマンドを CIMC GUI に表示することはできない
- CIMC GUI から CIMC CLI 出力を生成することはできない

CIMC GUI

CIMC GUI は、E シリーズ サーバおよびNCE用の Web ベース管理インターフェイスです。CIMC GUI を起動して、次の最小要件を満たしている任意のリモート ホストからサーバを管理できます。

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

CIMC GUI へのログイン

はじめる前に

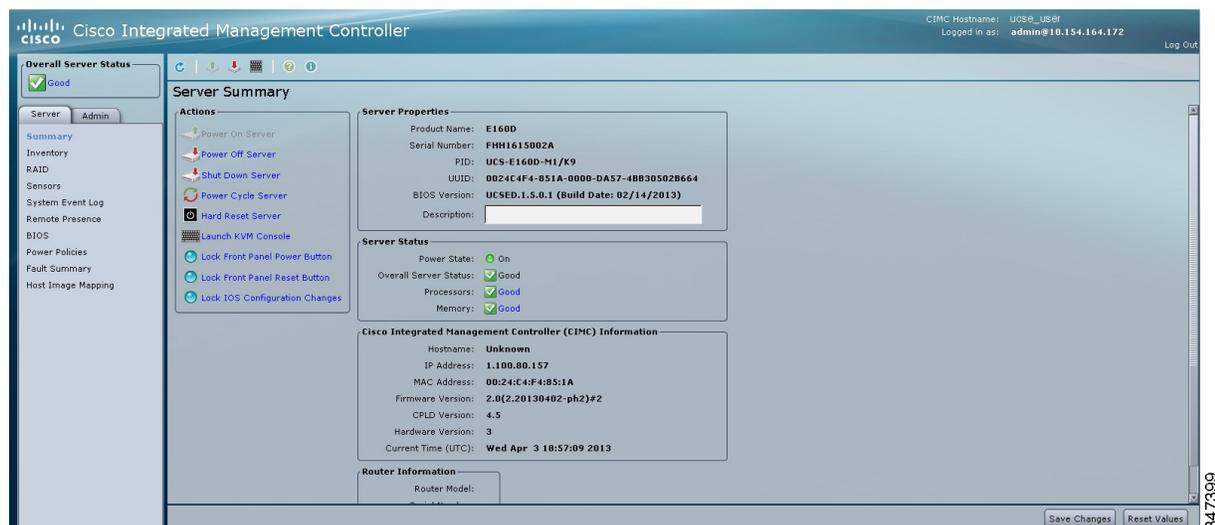
- CIMC にアクセスするための IP アドレスが設定済みであることを確認します。『*Getting Started Guide for Cisco UCS E-Series Server Modules*』の「*Configuring CIMC Access*」の章を参照してください。
- Adobe Flash Player 10 以降がインストールされていない場合は、ローカルマシンにインストールします。

手順

- ステップ 1** 初期セットアップ時に CIMC へのアクセス用に設定した IP アドレスを Web ブラウザに入力します。
- ステップ 2** セキュリティ ダイアログボックスが表示された場合は、次の操作を実行します。
- (任意) チェックボックスをオンにして、シスコからのすべてのコンテンツを受け入れます。
 - [Yes] をクリックして証明書を受け入れ、続行します。
- ステップ 3** ログイン ウィンドウで、ユーザ名とパスワードを入力します。
ヒント 未設定のシステムに初めてログインする場合は、ユーザ名に **admin**、パスワードに **password** を使用します。
- ステップ 4** [Log In] をクリックします。
[Change Password] ダイアログボックスが表示されます。
(注) [Change Password] ダイアログボックスは、CIMC に初めてログインしたときのみ表示されます。それ以降はリブートしても表示されません。
- ステップ 5** [New Password] フィールドに、新しいパスワードを入力します。
- ステップ 6** 確認のために [Confirm Password] フィールドにもう一度パスワードを入力します。
- ステップ 7** [Save Changes] をクリックします。
[Server Summary] ページが表示されます。このページが CIMC のホーム ページです。CIMC ホーム ページ、(5 ページ) を参照してください。

CIMC ホーム ページ

図 1: CIMC ホーム ページ



[Navigation] ペインと [Work] ペイン

[Navigation] ペインは、CIMC GUI の左側に表示されます。[Navigation] ペインの [Server] または [Admin] タブにあるリンクをクリックすると、右側の [Work] ペインに関連付けられたタブが表示されます。

[Navigation] ペインには次の領域があります。

- [Server] タブ
- [Admin] タブ

[Server] タブ

[Server] タブの各ノードは、[Work] ペインに表示される 1 つ以上のタブに続きます。これらのタブからは次の情報へアクセスできます。

[Server] タブのノード名	[Work] ペインのタブで提供される情報
変更点	サーバプロパティ、ステータス、BIOS のバージョン、CIMC ファームウェアのバージョン、IP アドレス、および MAC アドレス。
インベントリ	インストール済みの CPU、メモリカード、電源、PCI アダプタ。
RAID	ストレージアダプタおよびカード。
Sensor	温度、電圧、LED、およびストレージセンサーの読み取り。
システム イベント ログ	システム イベント メッセージ。
Remote Presence	LAN 設定上の KVM、仮想メディア、およびシリアル。
BIOS	インストール済みの BIOS ファームウェアバージョン、およびサーバのブート順。
Power Policies	電源ポリシーの設定。
Fault Summary	センサーの読み取りエラー。
ホスト イメージ マッピング	ホスト イメージのマッピング ステータスとイメージの情報。

[Admin] タブ

[Admin] タブの各ノードは、[Work] ペインに表示される 1 つ以上のタブに続きます。これらのタブからは次の情報へアクセスできます。

[Admin] タブのノード名	[Work] ペインのタブで提供される情報
User Management	ローカルで定義されたユーザ アカウント、Active Directory 設定、および現在のユーザ セッション情報。
ネットワーク	NIC、IPv4、VLAN、および LOM プロパティとネットワーク セキュリティ設定。
Communication Services	HTTP、SSH、XML API、IPMI over LAN のプロパティ。
Certificate Management	セキュリティ証明書情報と管理。
CIMC ログ	CIMC ログ メッセージ。
Event Management	プラットフォーム イベント フィルタ。
Firmware Management	CIMC ファームウェア情報と管理。
ユーティリティ	テクニカルサポートデータ収集、システム設定のインポートおよびエクスポート オプション。

ツールバー

ツールバーは [Work] ペインの上に表示されます。

エレメント名	説明
Refresh	現在のページを更新します。
Power On Server	サーバの電源を投入します。
Power Off Server	サーバの電源を切ります。
Launch KVM Console	KVM コンソールを起動します。
Help	ヘルプを表示します。
Info	CIMC 情報を表示します。

CIMC オンライン ヘルプ

CIMC ユーザ インターフェイスは、左側の [Navigation] ペインと右側の [Work] ペインの 2 つの主要なセクションに分かれています。ページに関するオンラインヘルプにアクセスするには、次のことを行います。

- ユーザ インターフェイスの特定のタブで、[?] アイコンをクリックします。[?] アイコンは、[Work] ペインの上方のツールバーにあります。
- ダイアログボックスにある [?] アイコンをクリックします。

CIMC GUI からのログアウト

手順

- ステップ 1** CIMC の右上で、[Log Out] をクリックします。
ログアウトすると、CIMC のログイン ページに戻ります。
- ステップ 2** (任意) 再度ログインするか、Web ブラウザを閉じます。
-



第 2 章

サーバ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、次の項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](#), 9 ページ
- [KVM コンソール](#), 10 ページ
- [PXE インストールサーバ](#), 13 ページ
- [ホストイメージマッピング](#), 15 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 シリーズサーバおよびNCE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
- ホストイメージマッピング



注意

仮想ドライブをマップするには 1 種類だけを使用する必要があります。たとえば、KVM コンソールまたは Host Image Mapping のいずれかを使用します。組み合わせて使用すると、サーバが未定義の状態になります。

KVM コンソール

KVM コンソールは CIMC からアクセス可能なインターフェイスであり、サーバへのキーボード、ビデオ、マウスの直接接続をエミュレートします。KVM コンソールを使用すると、リモートの場合からサーバに接続できます。サーバに物理的に接続された CD/DVD ドライブまたはフロッピー ドライブを使用する代わりに、KVM コンソールは仮想メディアを使用します。これは、仮想 CD/DVD ドライブまたはフロッピー ドライブにマップされる実際のディスク ドライブまたはディスク イメージ ファイルです。次のいずれでも仮想ドライブにマップできます。

- コンピュータ上の CD/DVD またはフロッピー ドライブ
- コンピュータ上のディスク イメージ ファイル (ISO または IMG ファイル)
- コンピュータ上の USB フラッシュ ドライブ

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

- ブートアップ中に F2 を押して、BIOS セットアップ メニューにアクセスします。
- ブートアップ中に F8 を押して、CIMC Configuration Utility にアクセスします。



(注) CIMC Configuration Utility は EHWIC E シリーズ NCE および NIM E シリーズ NCE には適用されません。

- Cisco UCS M1 および M2 サーバの場合は、ブートアップ中に Ctrl+H を押し、WebBIOS にアクセスして RAID を設定します。

Cisco UCS M3 サーバの場合は、ブートアップ中に Ctrl+R を押し、MegaRAID コントローラにアクセスして RAID を設定します。



(注) RAID は EHWIC E シリーズ NCE および NIM E シリーズ NCE ではサポートされていません。これらの SKU では、Ctrl+H および Ctrl+R は機能しません。

KVM コンソールを起動するための Java 要件

KVM コンソールを起動するためには、システムにリリース 1.6 以降の Java をインストールしておく必要があります。

証明書が Java で取り消されたために KVM コンソールが起動しない場合は、Java の設定を変更する必要があります。次の手順を実行します。

- 1 Java コントロール パネルにアクセスします。
- 2 [Advanced] タブをクリックします。

- 3 [Perform certificate revocation on] で、[Do not check (not recommended)] ラジオ ボタンを選択します。詳細については、http://www.java.com/en/download/help/revocation_options.xmlを参照してください。

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

はじめる前に

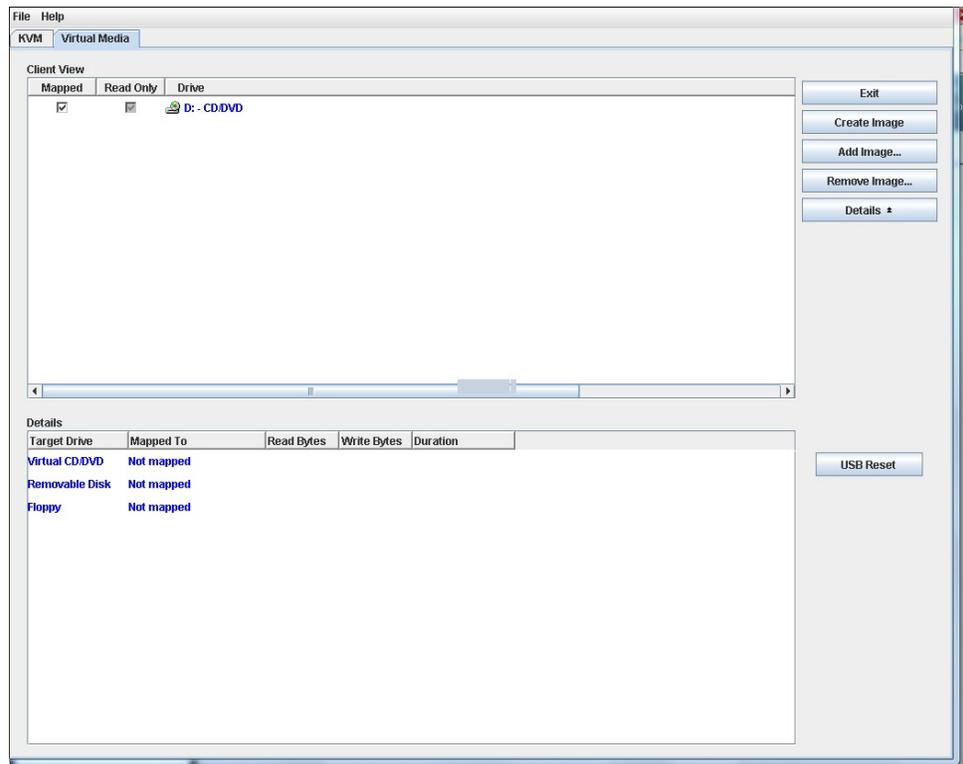
オペレーティングシステムまたはハイパーバイザのインストールディスクまたはディスクイメージファイルの場所を特定します。



- (注) VMware vSphere Hypervisor ではカスタマイズし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](#)、(14 ページ) を参照してください。

手順

- ステップ 1 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ディスクを CD/DVD ドライブにロードするか、ディスク イメージファイルをコンピュータにコピーします。
- ステップ 2 CIMC が開いていない場合は、CIMC GUI にログインします。
- ステップ 3 [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 4 作業ウィンドウの [Host Image Mapping] タブをクリックします。
- ステップ 5 [Actions] 領域から、[Launch KVM Console] をクリックします。
[KVM Console] が別ウィンドウで開きます。
- ステップ 6 KVM コンソールから、[Virtual Media] タブをクリックします。



ステップ 7 [Virtual Media] タブで、次のいずれかの方法を使用して仮想メディアをマップします。

- 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 ディスクが含まれている CD/DVD ドライブの [Mapped] チェックボックスをオンにします。
- [Add Image] をクリックし、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 ディスク イメージに移動してこれを選択します。[Open] をクリックしてディスク イメージをマウントし、マウントされたディスク イメージの [Mapped] チェックボックスをオンにします。

(注) インストールプロセスの実行中は、[Virtual Media] タブを開いたままにしておく必要があります。このタブを閉じると、すべての仮想メディアのマップが解除されます。

ステップ 8 仮想 CD/DVD ドライブがブート デバイスになるように、ブート順を設定します。

ステップ 9 サーバをリブートします。

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

ステップ 10 オペレーティングシステムまたはハイパーバイザをインストールした後にディスク ドライブが表示されない場合は、ドライバをインストールする必要があります。ドライバのインストール手順については、該当するオペレーティング システムまたはハイパーバイザのマニュアルを参照してください。

Microsoft Windows オペレーティング システムへのドライバのインストール手順については、[Microsoft Windows Server 用のドライバのインストール](#)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、仮想メディアのブート順を元の設定にリセットします。

PXE インストール サーバ

Preboot Execution Environment (PXE) インストール サーバを使用すると、クライアントはリモートの場所からオペレーティング システムまたはハイパーバイザをブートおよびインストールできます。この方法を使用するには、PXE 環境が設定されていて、VLAN (通常は専用のプロビジョニング VLAN) で使用できるようになっている必要があります。さらに、サーバがネットワークからブートするように設定されている必要があります。サーバは、ブートすると、PXE 要求をネットワーク経由で送信します。PXE インストール サーバは、この要求に応答確認し、サーバにオペレーティング システムまたはハイパーバイザをインストールするイベントのシーケンスを開始します。

PXE サーバは、インストールディスク、ディスクイメージ、またはスクリプトを使用して、オペレーティング システムまたはハイパーバイザをインストールできます。また、独自のディスクイメージを使用して、プラットフォーム、追加コンポーネント、またはアプリケーションをインストールすることもできます。



(注) PXE インストールは、多数のサーバにプラットフォームをインストールする場合に効率のよい方法です。ただし、この方法を使用するには PXE 環境をセットアップする必要があることを考えると、他のインストール方法を使用する方が簡単な場合があります。

PXE インストールサーバを使用したオペレーティング システムまたはハイパーバイザのインストール

はじめる前に

VLAN 経由でサーバに到達できることを確認します。



(注) VMware vSphere Hypervisor ではカスタマイズし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](#)、(14 ページ) を参照してください。

手順

ステップ 1 ブート順を [PXE] に設定します。

ステップ 2 サーバをリブートします。

注意 共有 LOM インターフェイスを使用して CIMC にアクセスしている場合は、サーバのリブートプロセス中に CIMC GUI を使用しないでください。CIMC GUI を使用すると、イーサネットポートに設定されていた IP アドレスがブートエージェントによってオーバーライドされるため、PXE のインストール中に GUI の接続が解除されます。

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ール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。

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

手順

ステップ 1 <https://my.vmware.com/web/vmware/login> にアクセスします。

VMware ログイン ページが表示されます。

ステップ 2 自分の VMware クレデンシャルを入力し、[Log In] をクリックします。

VMware のアカウントがない場合は、[Register] をクリックして無料アカウントを作成します。

ステップ 3 [Downloads] をクリックし、ドロップダウン リストから [All Products] を選択します。

ステップ 4 必要に応じて、次のいずれかを実行します。

- VMware vSphere Hypervisor 5.1 イメージをダウンロードするには、[Search] フィールドで ESXi-5.1.0-799733-custom-Cisco-2.1.0.3.iso と入力し、[Search] アイコンをクリックします。[Search Results] から [VMware vSphere] > [Drivers & Tools] > [Cisco Custom Image for ESXi 5.1.0 GA Install CD] をクリックし、[Download] をクリックします。
- VMware vSphere Hypervisor 5.5 イメージをダウンロードするには、[Search] フィールドで ESXi-5.5.0-1331820-custom-Cisco-5.5.0.1.iso と入力し、[Search] アイコンをクリックします。[Search Results] から [VMware vSphere] > [Drivers & Tools] > [CISCO Custom Image for ESXi 5.5.0 GA Install CD] をクリックし、[Download] をクリックします。

次の作業

VMware vSphere Hypervisor のイメージをインストールします。

ホストイメージマッピング

ホストイメージマッピング機能を使用すると、ホストイメージのダウンロード、マッピング、マッピング解除、または削除を行うことができます。Microsoft Windows、Linux、VMware などのホストイメージを、リモート FTP または HTTP サーバから CIMC 内部リポジトリにダウンロードしてから、E シリーズサーバまたは NCE 内の USB コントローラの仮想ドライブにマップします。イメージをマップした後は、イメージをマウントした仮想ドライブが最初のブートデバイスになるようにブート順序を設定してから、サーバをリブートします。ホストイメージはファイル拡張子として .iso または .img がなければなりません。

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

ホストイメージのマッピング

はじめる前に

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



(注) VMware vSphere Hypervisor ではカスタマイズし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](#)、(14 ページ) を参照してください。



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

手順

- ステップ 1 [Navigation] ペインの [Compute] メニューをクリックします。
- ステップ 2 作業ウィンドウの [Host Image Mapping] タブをクリックします。
- ステップ 3 [Host Image Mapping] ページで、[Add Image] をクリックします。
[Add New Mapping] ダイアログボックスが表示されます。次のフィールドに入力します。

名前	説明
[Server Type] ドロップダウン リスト	<p>イメージが配置されているリモートサーバのタイプ。次のいずれかになります。</p> <ul style="list-style-type: none"> • FTP • FTPS • HTTP • HTTPS <p>(注) 選択したリモートサーバによって、表示されるフィールドが変わります。</p>
[Server IP Address] フィールド	<p>リモート FTP または HTTP サーバの IP アドレス。</p>
[File Path] フィールド	<p>リモート FTP または HTTP サーバのパスおよびファイル名。パスワードには、最大 80 文字を使用できます。</p> <ul style="list-style-type: none"> • ホストイメージをインストールする場合、そのイメージのファイル拡張子は必ず <code>.iso</code> または <code>.img</code> になります。 • 診断イメージをインストールする場合、そのイメージのファイル拡張子は必ず <code>.diag</code> になります。
[Username] フィールド	<p>リモート サーバのユーザ名。</p> <p>ユーザ名は 1~20 文字の範囲で指定します。</p> <p>(注) ユーザ名を設定しない場合は、ユーザ名として <code>anonymous</code> を入力し、パスワードとして任意の文字を入力します。</p>
[Password] フィールド	<p>ユーザ名のパスワード。</p> <p>パスワードは 1~20 文字の範囲で指定します。</p> <p>(注) ユーザ名を設定しない場合は、ユーザ名として <code>anonymous</code> を入力し、パスワードとして任意の文字を入力します。</p>

ステップ 4 [Download] をクリックします。
 [Host Image Mapping] ページが開きます。[Host Image Mapping Status] 領域で、イメージダウンロードのステータスを表示できます。イメージが正常にダウンロードされ、処理された後、ページがリフレッシュされます。ページがリフレッシュされた後、新しいイメージが [Image Information] 領域に表示されます。

ステップ 5 [Image Information] 領域で、マップするイメージを選択し、[Map Selected Image] をクリックします。

イメージがマップされ、USB コントローラの仮想ドライブにマウントされます。仮想ドライブには、次のいずれかを使用できます。

- HDD : ハードディスク ドライブ
- FDD : フロッピー ディスク ドライブ
- CD/DVD : ブート可能 CD-ROM または DVD ドライブ

ステップ 6 イメージがマウントされている仮想ドライブが最初のブートデバイスになるように、ブート順を設定します。

ヒント イメージがどの仮想ドライブにマウントされているか確認するには、[Host Image Mapping] ページの [Host Image Update Status] 領域を参照してください。

ステップ 7 サーバをリブートします。

ステップ 8 イメージにアンサーファイルが含まれている場合、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自動化され、イメージがインストールされます。そうでない場合は、インストールウィザードが表示されます。ウィザードの手順に従って、イメージをインストールします。

ステップ 9 オペレーティングシステムまたはハイパーバイザをインストールした後にディスクドライブが表示されない場合は、ドライブをインストールする必要があります。ドライブのインストール手順については、該当するオペレーティングシステムまたはハイパーバイザのマニュアル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、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

ステップ 1 [Navigation] ペインの [Compute] メニューをクリックします。

ステップ 2 作業ウィンドウの [Host Image Mapping] タブをクリックします。

ステップ 3 作業ウィンドウの [Host Image Mapping] タブをクリックします。

ステップ 4 [Unmap Image] をクリックします。

USB コントローラの仮想ドライブから、マップされたイメージがアンマウントされます。

ホストイメージの削除

はじめる前に

admin 権限を持つユーザとして CIMC にログインします。

手順

- ステップ 1 [Navigation] ペインの [Compute] メニューをクリックします。
 - ステップ 2 作業ウィンドウの [Host Image Mapping] タブをクリックします。
 - ステップ 3 [Current Mappings Information] 領域で、削除するイメージを選択します。
 - ステップ 4 [Delete Selected Image] をクリックします。
イメージが SD カードから削除されます。
-



第 3 章

サーバの管理

この章は、次の項で構成されています。

- [全体のサーバステータスの表示, 19 ページ](#)
- [CIMC GUI を使用したサーバのブート順の設定, 21 ページ](#)
- [BIOS セットアップ メニューを使用したブート順の設定, 24 ページ](#)
- [サーバのリセット, 25 ページ](#)
- [サーバのシャットダウン, 25 ページ](#)
- [Cisco IOS CLI 設定変更のロックまたはロック解除, 26 ページ](#)
- [サーバの電源管理, 27 ページ](#)
- [BIOS の設定, 32 ページ](#)
- [トラステッドプラットフォーム モジュールの設定, 49 ページ](#)

全体のサーバステータスの表示

手順

- ステップ 1** [Navigation] ペインの [Overall Server Status] 領域で、青色のヘルス レポート リンクをクリックして、[Server Summary] ペインを更新します。
- ステップ 2** (任意) [Server Summary] ペインの [Server Status] 領域で次の情報を確認します。
(注) 次に、表示される可能性のあるすべてのステータス フィールドを示します。実際に表示されるフィールドは、使用している E シリーズサーバのタイプによって異なります。

名前	説明
[Power State] フィールド	現在の電源状態。

名前	説明
[Overall Server Status] フィールド	<p>サーバの全体的なステータス。次のいずれかになります。</p> <ul style="list-style-type: none"> • [Memory Test In Progress] : サーバは搭載されているメモリのセルフテストを実行しています。この状態は、通常、ブートプロセスの間に発生します。 • Good • Moderate Fault • Severe Fault
[Temperature] フィールド	<p>温度ステータス。次のいずれかになります。</p> <ul style="list-style-type: none"> • Good • Fault • Severe Fault <p>このフィールドのリンクをクリックして、詳細な温度情報を表示できます。</p>
[Processors] フィールド	<p>プロセッサの全体的なステータス。次のいずれかになります。</p> <ul style="list-style-type: none"> • Good • Fault <p>このフィールドのリンクをクリックして、プロセッサに関する詳細情報を表示できます。</p>
[Memory] フィールド	<p>メモリモジュールの全体的なステータス。次のいずれかになります。</p> <ul style="list-style-type: none"> • Good • Fault • Severe Fault <p>このフィールドのリンクをクリックして、詳細なステータス情報を表示できます。</p>

名前	説明
[Overall DIMM Status] フィールド	<p>DIMM モジュールの全体的なステータス。次のいずれかになります。</p> <ul style="list-style-type: none"> • Good • Fault • Severe Fault <p>このフィールドのリンクをクリックして、詳細なステータス情報を表示できます。</p>
[Overall Storage Status] フィールド	<p>すべてのコントローラの全体的なステータス。次のいずれかになります。</p> <ul style="list-style-type: none"> • Good • Moderate Fault • Severe Fault <p>このフィールドのリンクをクリックして、詳細なステータス情報を表示できます。</p>

CIMC GUI を使用したサーバのブート順の設定

はじめる前に

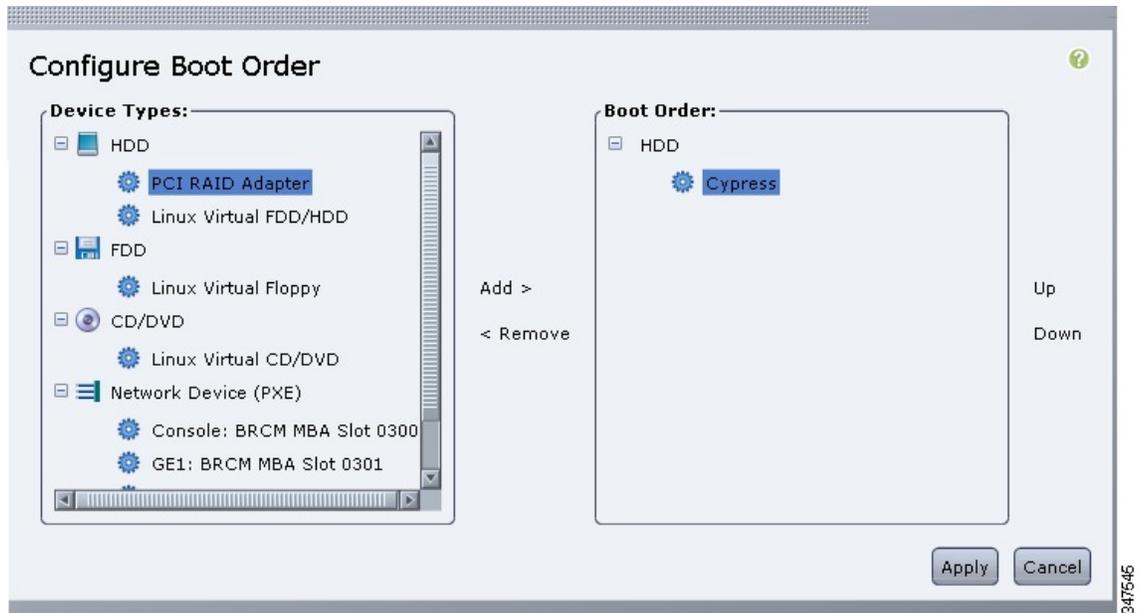
admin 権限を持つユーザとして CIMC にログインします。

手順

- ステップ 1 [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2 [Server] タブの [BIOS] をクリックします。
- ステップ 3 [Actions] 領域で、[Configure Boot Order] をクリックします。

[Configure Boot Order] ダイアログボックスが表示されます。

図 2 : [Configure Boot Order] ダイアログボックス



ステップ 4 [Configure Boot Order] ダイアログボックスで、必要に応じて次のフィールドに値を入力します。

名前	説明
[Device Types] テーブル	<p>サーバのブート オプション。次のものがあります。</p> <ul style="list-style-type: none"> • HDD : ハードディスク ドライブ。次のオプションがあります。 <ul style="list-style-type: none"> ◦ キプロス ◦ PCI RAID アダプタ ◦ Linux 仮想 FDD/HDD ◦ SSD ハードドライブ • FDD : フロッピー ディスク ドライブ。次のオプションがあります。 <ul style="list-style-type: none"> ◦ Linux 仮想フロッピー • CD/DVD : ブート可能 CD-ROM。次のオプションがあります。 <ul style="list-style-type: none"> ◦ Linux 仮想 CD/DVD • ネットワーク デバイス (PXE) : PXE ブート。次のオプションがあります。 <ul style="list-style-type: none"> ◦ コンソール ◦ GE1 ◦ GE2 ◦ GE3 ◦ TE2 ◦ TE3 <p>(注) PXE ブート オプションは、プラットフォームによって異なります。たとえば、M3サーバでは、GE2 と GE3 の代わりに、TE2 と TE3 を使用します。</p> • 内部 EFI シェル : 内部 Extensible Firmware Interface。
Add >	選択したデバイス タイプを [Boot Order] テーブルに移動します。
< Remove	選択したデバイス タイプを [Boot Order] テーブルから削除します。

名前	説明
[Boot Order] テーブル	このサーバがブートできるデバイスタイプが、ブートが試行される順番に表示されます。
Up	選択したデバイス タイプを [Boot Order] テーブルで高いプライオリティに移動します。
Down	選択したデバイス タイプを [Boot Order] テーブルで低いプライオリティに移動します。

- ステップ 5** [Apply] をクリックします。
サーバに接続しているデバイスによっては、実際のブート順に追加のデバイス タイプが付加される場合があります。

次の作業

サーバを再起動して、新しいブート順でブートします。

BIOS セットアップメニューを使用したブート順の設定

E シリーズ サーバまたは NCE に直接接続されている USB や外部 CD ROM ドライブなど、外部のブート可能なデバイスからサーバをブートするには、次の手順を実行します。

手順

- ステップ 1** [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2** 作業ウィンドウの [Host Image Mapping] タブをクリックします。
- ステップ 3** [Actions] 領域から、[Launch KVM Console] をクリックします。
[KVM Console] が別ウィンドウで開きます。
- ステップ 4** [Server Summary] ページから、[Power Cycle Server] をクリックしてサーバをリブートします。
- ステップ 5** プロンプトが表示されたら、ブートアップが完了する前に F2 を押して BIOS セットアップメニューにアクセスします。
[Aptio Setup Utility] が表示されます。このユーティリティから、BIOS セットアップメニューのオプションを利用できます。
- ステップ 6** [Boot] タブをクリックします。
- ステップ 7** [Boot Options Priority] 領域の下のページを一番下までスクロールします。次のブート オプション
プライオリティが一覧表示されます。
- Floppy Drive BBS Priorities

- Network Device BBS Priorities
- Hard Drive BBS Priorities
- CD/DVD ROM Drive BBS Priorities

- ステップ 8** キーボードの上矢印キーまたは下矢印キーを使用して、適切なオプションを強調表示します。
- ステップ 9** Enter を押して、強調表示されているフィールドを選択します。
- ステップ 10** [Boot Option 1] に適切なデバイスを選択します。
- ステップ 11** F4 を押して変更を保存し、終了します。
BIOS セットアップの [Main] タブに、[Boot Option 1] として設定したデバイスが表示されます。
-

サーバのリセット

はじめる前に

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

手順

- ステップ 1** [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2** 作業ウィンドウの [Host Image Mapping] タブをクリックします。
- ステップ 3** [Actions] 領域で、[Hard Reset Server] をクリックします。
[Hard Reset the Server?] というメッセージが示されたダイアログボックスが表示されます。
- ステップ 4** [OK] をクリックします。
-

サーバのシャットダウン

はじめる前に

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

手順

-
- ステップ 1** [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2** 作業ウィンドウの [Host Image Mapping] タブをクリックします。
- ステップ 3** [Actions] 領域で、[Shut Down Server] をクリックします。
[Shut Down the Server?] というメッセージを含むダイアログボックスが表示されます。
- (注) [Shut Down Server] をクリックした場合、または E シリーズ サーバの前面パネルにある電源ボタンを押した場合、Citrix XenServer はグレースフル シャットダウンしません。
- ステップ 4** [OK] をクリックします。
- (注) NIM E シリーズ NCE のシャットダウンには最大 60 秒かかります。シャットダウンを 2、3 回試しても NIM E シリーズ NCE がシャットダウンしない場合は、ルータから次のコマンドを入力します。
- 1 Router # hw-module subslot 0/NIM-slot-number stop
 - 2 Router # hw-module subslot 0/NIM-slot-number start
-

Cisco IOS CLI 設定変更のロックまたはロック解除

この手順を使用して、Cisco IOS CLI を使用した設定変更を許可または禁止します。

はじめる前に

- admin 権限を持つユーザとして CIMC にログインします。

手順

-
- ステップ 1** [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2** 作業ウィンドウの [Host Image Mapping] タブをクリックします。
- ステップ 3** Cisco IOS CLI を使用した設定変更を許可するには、[Actions] 領域で [Unlock IOS Configuration Changes] をクリックします。
GUI のボタンが [Lock IOS Configuration Changes] に変わります。
- ステップ 4** Cisco IOS CLI を使用した設定変更を禁止するには、[Actions] 領域で [Lock IOS Configuration Changes] をクリックします。
Cisco IOS CLI を使用して設定を変更すると、警告メッセージが表示され、その設定は無視されま

GUI のボタンが [Unlock IOS Configuration Changes] に変わります。

ステップ 5 確認ウィンドウで、[OK] をクリックします。

サーバの電源管理

サーバの電源投入



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

はじめる前に

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

手順

- ステップ 1** [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2** 作業ウィンドウの [Host Image Mapping] タブをクリックします。
- ステップ 3** [Actions] 領域で、[Power On Server] をクリックします。
[Power on the server?] というメッセージが示されたダイアログボックスが表示されます。
- ステップ 4** [OK] をクリックします。

サーバの電源オフ



(注) この手順は NIM E シリーズ NCE には適用されません。

はじめる前に

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

手順

-
- ステップ 1** [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2** 作業ウィンドウの [Host Image Mapping] タブをクリックします。
- ステップ 3** [Actions] 領域で、[Power Off Server] をクリックします。
[Power Off the Server?] というメッセージを含むダイアログボックスが表示されます。
- ステップ 4** [OK] をクリックします。
- (注) NIM E シリーズ NCE の場合は、[Shut Down Server] をクリックすることをお勧めします。電源を切る必要がある場合は、ルータで次のコマンドを使用します。
- 1 Router # hw-module subslot 0/NIM-slot-number stop
 - 2 Router # hw-module subslot 0/NIM-slot-number start
-

サーバ電源の再投入



(注) この手順は NIM E シリーズ NCE には適用されません。

はじめる前に

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

手順

-
- ステップ 1** [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2** 作業ウィンドウの [Host Image Mapping] タブをクリックします。
- ステップ 3** [Actions] 領域で、[Power Cycle Server] をクリックします。
[Power Cycle the Server?] というメッセージを含むダイアログボックスが表示されます。
- ステップ 4** [OK] をクリックします。
- (注)
- サーバ電源の再投入は、サーバの物理的な電源ボタンを押して電源をオフにした後に、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。

(注) NIM E シリーズ NCE の場合は、[Shut Down Server] をクリックすることをお勧めします。電源を再投入する必要がある場合は、ルータで次のいずれかのコマンドを使用します。

- 1 Router # hw-module subslot 0/NIM-slot-number stop
- 2 Router # hw-module subslot 0/NIM-slot-number start
- Router # hw-module subslot 0/NIM-slot-number reload

(注) このコマンドにより、モジュールの電源が再投入されます。CIMC とサーバがリブートします。

電力復元ポリシーの設定

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

はじめる前に

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



(注) NIM では、CIMC 3.1.x GUI から電源復元ポリシー オプションを設定できません。他の設定方法 (CLI、XMLAPI) を使用する必要があります。CIMC 3.2.x では、GUI などのすべての設定方法がサポートされています。



(注) この機能は、ISR 4K ルータでのみサポートされます。ISR G2 ではサポートされません。ISR G2 の場合は、CIMC の BIOS 設定を参照してください。

手順

- ステップ 1 [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2 [Server] タブの [Power Policies] をクリックします。
- ステップ 3 [Power Restore Policy] 領域で、次のフィールドを更新します。

名前	説明
[Power Restore Policy] ドロップ ダウン リスト	<p>予期しない電源損失後、シャーン電源が復元されたときに実行されるアクション。次のいずれかになります。</p> <ul style="list-style-type: none"> • [Power Off] : 手動で再起動されるまで、サーバはオフのままです。 • [Power On] : 電源が復元されたときに、サーバは通常どおりに起動できます。 • [Restore Last State] : サーバを電源損失前と同じ電源状態（オフまたはオン）に復元します。これがデフォルトのアクションになります。

ステップ 4 [Save Changes] をクリックします。

サーバの前面パネルにある電源ボタンのロックまたはロック解除



(注) この手順はE シリーズサーバおよびSME シリーズNCE に適用されます。この手順はEHWIC E シリーズNCE およびNIM E シリーズNCE には適用されません。

この手順を使用して、物理サーバの前面パネルにある物理的な電源ボタンを有効または無効にします。

はじめる前に

- admin 権限を持つユーザとして CIMC にログインします。
- サーバの電源を切ります。

手順

- ステップ 1 [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2 作業ウィンドウの [Host Image Mapping] タブをクリックします。
- ステップ 3 電源ボタンを無効にするには、[Actions] 領域で [Lock Front Panel Power Button] をクリックします。電源ボタンが無効になります。前面パネルの電源ボタンを使用して、サーバの電源をオンまたはオフにすることはできません。

GUI のボタンが [Unlock Front Panel Power Button] に変わります。

- ステップ 4** 電源ボタンを有効にするには、[Actions] 領域で [Unlock Front Panel Power Button] をクリックします。
電源ボタンが有効になります。サーバの電源をオンまたはオフにするには、前面パネルの電源ボタンを使用できます。

GUI のボタンが [Lock Front Panel Power Button] に変わります。

- ステップ 5** 確認ウィンドウで、[OK] をクリックします。

サーバの前面パネルにあるリセットボタンのロックまたはロック解除



- (注) この手順は E シリーズ サーバおよび SME シリーズ NCE に適用されます。この手順は EHWIC E シリーズ NCE および NIM E シリーズ NCE には適用されません。

この手順を使用して、物理サーバの前面パネルにあるリセット ボタンを有効または無効にします。

はじめる前に

- admin 権限を持つユーザとして CIMC にログインします。
- サーバの電源を切ります。

手順

- ステップ 1** [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2** 作業ウィンドウの [Host Image Mapping] タブをクリックします。
- ステップ 3** リセット ボタンを無効にするには、[Actions] 領域で [Lock Front Panel Reset Button] をクリックします。
リセットボタンが無効になります。前面パネルのリセットボタンを使用して、サーバをリセットすることはできません。
GUI のボタンが [Unlock Front Panel Reset Button] に変わります。
- ステップ 4** リセット ボタンを有効にするには、[Actions] 領域で [Unlock Front Panel Reset Button] をクリックします。
リセットボタンが有効になります。前面パネルのリセットボタンを使用して、サーバをリセットできます。

GUI のボタンが [Lock Front Panel Reset Button] に変わります。

ステップ 5 確認ウィンドウで、[OK] をクリックします。

BIOS の設定

バックアップ BIOS のアクティブ化

まれにですが、BIOS イメージは破損することがあります。破損した BIOS イメージから回復するには、バックアップ BIOS をアクティブにしてシステムをブートします。



(注) バックアップ BIOS イメージは、工場出荷時にインストール済みです。アップグレードすることはできません。

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

-
- ステップ 1 [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2 [Server] タブの [BIOS] をクリックします。
- ステップ 3 [Actions] 領域で、[Activate Backup BIOS] をクリックします。
- ステップ 4 確認ウィンドウで、[OK] をクリックします。
-

BIOS の詳細設定



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

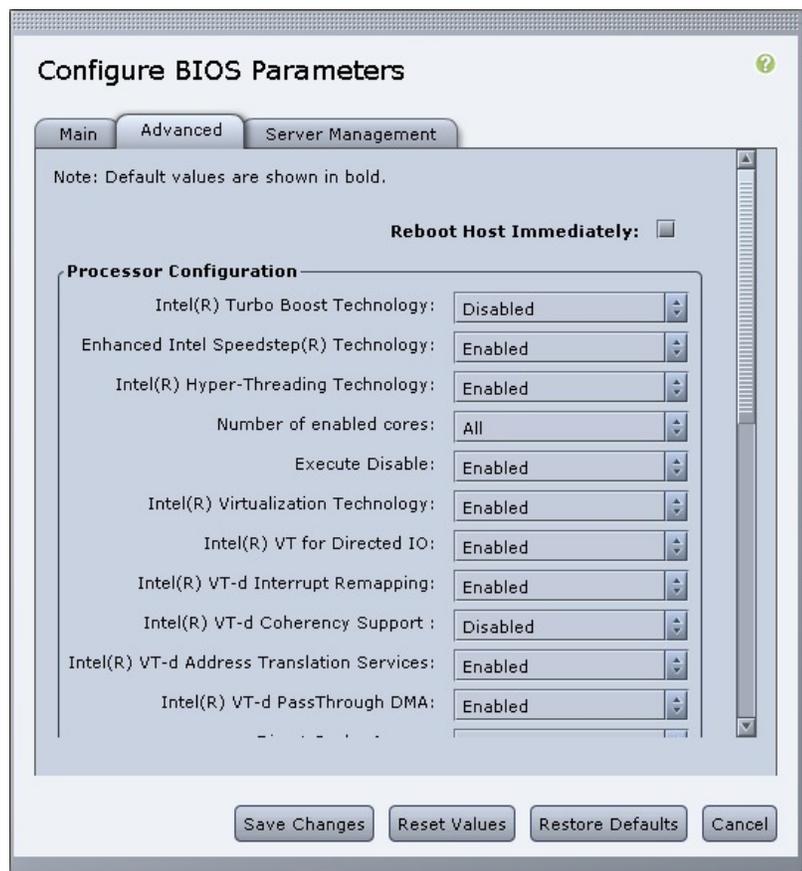
はじめる前に

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

手順

- ステップ1 [Navigation] ペインの [Server] メニューをクリックします。
- ステップ2 [Server] タブの [BIOS] をクリックします。
- ステップ3 [Actions] 領域で [Configure BIOS] をクリックします。
[Configure BIOS Parameters] ダイアログボックスが表示されます。
- ステップ4 [Configure BIOS Parameters] ダイアログボックスで、[Advanced] タブをクリックします。

図 3: [Advanced] タブ



- ステップ5 [Reboot Host Immediately] チェックボックスをオンまたはオフにします。
オンにすると、BIOS パラメータの変更後、サーバがただちにリブートされます。
サーバが自動ではリブートしないように指定するには、このチェックボックスをオフにします。
パラメータの変更は、サーバが次にリブートされたときに有効になります。

(注) この手順は NIM E シリーズ NCE には適用されません。

- ステップ 6 [Advanced] タブで、BIOS 設定のフィールドを更新します。
 - ステップ 7 [Save Changes] をクリックします。
-

サーバ管理 BIOS の設定

はじめる前に

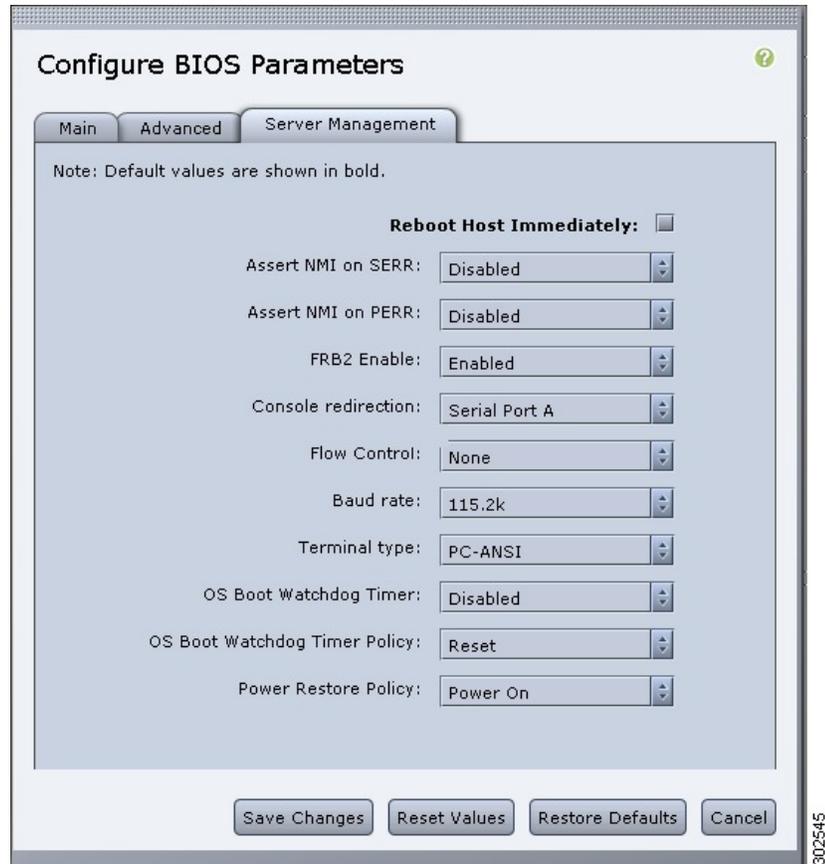
このタスクを実行するには、admin 権限を持つユーザとしてログインする必要があります。

手順

- ステップ 1 [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2 [Server] タブの [BIOS] をクリックします。
- ステップ 3 [Actions] 領域で [Configure BIOS] をクリックします。
[Configure BIOS Parameters] ダイアログボックスが表示されます。

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

図 4 : [Server Management] タブ



ステップ 5 [Reboot Host Immediately] チェックボックスをオンまたはオフにします。オンにすると、BIOS パラメータの変更後、サーバがただちにリブートされます。

サーバが自動ではリブートしないように指定するには、このチェックボックスをオフにします。パラメータの変更は、サーバが次にリブートされたときに有効になります。

(注) この手順は NIM E シリーズ NCE には適用されません。

ステップ 6 [Server Management] タブで、BIOS 設定のフィールドを更新します。

ステップ 7 [Save Changes] をクリックします。

BIOS CMOS のクリア



(注) 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。

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。
- サーバの電源を切ります。

手順

- ステップ 1 [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2 [Server] タブの [BIOS] をクリックします。
- ステップ 3 [Actions] 領域の [Clear BIOS CMOS] をクリックします。
- ステップ 4 確認ウィンドウで、[OK] をクリックします。

BIOS パスワードのクリア

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

- ステップ 1 [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2 [Server] タブの [BIOS] をクリックします。
- ステップ 3 [Actions] 領域の [Clear BIOS Password] をクリックします。
- ステップ 4 確認ウィンドウで、[OK] をクリックします。

次の作業

パスワードのクリア操作を反映させるために、サーバをリブートします。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。

サーバ BIOS 設定

次の各表に、表示および設定が可能なサーバ BIOS 設定を示します。



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

メイン BIOS 設定

名前	説明
[Reboot Host Immediately] NIM E シリーズ NCE には表示されません。	オンにすると、[Save Changes] をクリックした後ただちにサーバがリブートされます。 サーバが自動ではリブートしないように指定するには、このチェックボックスをオフにします。パラメータの変更は、サーバが次にリブートされたときに有効になります。

詳細：プロセッサ BIOS 設定

名前	説明
[Intel Turbo Boost Technology] [Intel Turbo Boost Technology]	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。 <ul style="list-style-type: none"> • [Disabled]：プロセッサの周波数は自動的に上がりません。 • [Enabled]：必要に応じてプロセッサで Turbo Boost Technology が利用されます。

名前	説明
[Enhanced Intel Speedstep Technology]	<p>プロセッサで Enhanced Intel SpeedStep Technology を使用するかどうか。このテクノロジーでは、プロセッサの電圧やコア周波数をシステムが動的に調整できます。このテクノロジーにより、平均電力消費量と平均熱発生量が減少する可能性があります。次のいずれかになります。</p> <ul style="list-style-type: none"> • [Disabled] : プロセッサの電圧または周波数を動的に調整しません。 • [Enabled] : プロセッサで Enhanced Intel SpeedStep Technology が使用され、サポートされているすべてのスリープ状態でさらに電力を節約することが可能になります。 <p>オペレーティングシステムがこの機能をサポートするかどうかについては、オペレーティングシステムのベンダーに問い合わせることを推奨します。</p>
[Intel Hyper-Threading Technology]	<p>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。</p> <ul style="list-style-type: none"> • [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。 <p>オペレーティングシステムがこの機能をサポートするかどうかについては、オペレーティングシステムのベンダーに問い合わせることを推奨します。</p>

名前	説明
[Number of Enabled Cores]	<p>パッケージ内の論理プロセッサ コアの状態を設定します。この設定をディセーブルにすると、ハイパースレッディングもディセーブルになります。次のいずれかになります。</p> <ul style="list-style-type: none"> • [All] : すべての論理プロセッサ コアでマルチ プロセッシングをイネーブルにします。 • [1] ~ [n] : サーバ上で動作できる論理プロセッサ コアの数を指定します。マルチプロセッシングをディセーブルにし、サーバ上で動作する論理プロセッサ コアを1つだけにするには、[1] を選択します。 <p>オペレーティングシステムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。</p>
[Execute Disable]	<p>アプリケーションコードを実行できる場所を指定するために、サーバのメモリ領域を分類します。この分類の結果、悪意のあるワームがバッファにコードを挿入しようとした場合、プロセッサでコードの実行をディセーブルにします。この設定は、損害、ワームの増殖、および特定クラスの悪意のあるバッファオーバーフロー攻撃を防止するのに役立ちます。次のいずれかになります。</p> <ul style="list-style-type: none"> • [Disabled] : プロセッサでメモリ領域を分類しません。 • [Enabled] : プロセッサでメモリ領域を分類します。 <p>オペレーティングシステムがこの機能をサポートするかどうかについては、オペレーティング システムのベンダーに問い合わせることを推奨します。</p>

名前	説明
[Intel Virtualization Technology]	<p>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。</p> <ul style="list-style-type: none"> • [Disabled] : プロセッサでの仮想化を禁止します。 • [Enabled] : プロセッサで、複数のオペレーティングシステムをそれぞれ独立したパーティション内で実行できます。 <p>(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。</p>
[Intel VT for Directed IO]	<p>Intel Virtualization Technology for Directed I/O (VT-d) をプロセッサで使用するかどうか。次のいずれかになります。</p> <ul style="list-style-type: none"> • [Disabled] : プロセッサで仮想化テクノロジーを使用しません。 • [Enabled] : プロセッサで仮想化テクノロジーを使用します。
[Intel VT-d Interrupt Remapping]	<p>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。</p> <ul style="list-style-type: none"> • [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]	<p>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。</p> <ul style="list-style-type: none"> • [Disabled] : プロセッサでコヒーレンス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]	<p>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。</p> <ul style="list-style-type: none"> • [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]	<p>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。</p> <ul style="list-style-type: none"> • [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]	<p>プロセッサで、データを I/O デバイスから直接プロセッサ キャッシュに入れることにより、I/O パフォーマンスを向上させることができます。この設定はキャッシュミスが減らすのに役立ちます。次のいずれかになります。</p> <ul style="list-style-type: none"> • [Disabled] : データは I/O デバイスから直接プロセッサ キャッシュには入れられません。 • [Enabled] : データは I/O デバイスから直接プロセッサ キャッシュに入れられます。
[Processor C3 Report]	<p>プロセッサからオペレーティング システムに C3 レポートを送信するかどうか。次のいずれかになります。</p> <ul style="list-style-type: none"> • [Disabled] : プロセッサから C3 レポートを送信しません。 • [ACPI C2][ACPI_C2] : C2 フォーマットを使用してプロセッサから C3 レポートを送信します。 • [ACPI C3][ACPI_C3] : C3 フォーマットを使用してプロセッサから C3 レポートを送信します。

名前	説明
[Processor C6 Report]	<p>プロセッサからオペレーティング システムに C6 レポートを送信するかどうか。次のいずれかになります。</p> <ul style="list-style-type: none"> • [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]	<p>プロセッサで、インテルハードウェアプリフェッチャが必要に応じてデータおよび命令ストリームをメモリから取得し、統合 2 次キャッシュに入れることを許可するかどうか。次のいずれかになります。</p> <ul style="list-style-type: none"> • [Disabled] : ハードウェアプリフェッチャは使用しません。 • [Enabled] : プロセッサで、キャッシュの問題が検出されたときにプリフェッチャを使用します。 <p>(注) この値を設定するには、[CPU Performance] ドロップダウンリストで [Custom] を選択する必要があります。[Custom] 以外の値の場合は、このオプションよりも、選択された CPU パフォーマンス プロファイルの設定が優先されます。</p>
[Adjacent Cache-Line Prefetch]	<p>プロセッサで、Intel Adjacent Cache-Line Prefetch メカニズムを使用して必要に応じてデータを取得するかどうか。次のいずれかになります。</p> <ul style="list-style-type: none"> • [Disabled] : Adjacent Cache-Line Prefetch メカニズムは使用しません。 • [Enabled] : キャッシュの問題が検出されたときに Adjacent Cache-Line Prefetch メカニズムを使用します。 <p>(注) この値を設定するには、[CPU Performance] ドロップダウンリストで [Custom] を選択する必要があります。[Custom] 以外の値の場合は、このオプションよりも、選択された CPU パフォーマンス プロファイルの設定が優先されます。</p>

名前	説明
[Package C State Limit]	<p>アイドル時にサーバ コンポーネントが使用できる電力量。次のいずれかになります。</p> <ul style="list-style-type: none"> • [C0 state][C0_state] : サーバはすべてのサーバ コンポーネントに常にフルパワーを提供します。このオプションでは、最高レベルのパフォーマンスが維持され、最大量の電力が必要となります。 • [C2 state][C2_state] : システム レベルの調整が進行中のため、電力消費が多くなります。調整が完了するまで、パフォーマンス上の問題が発生する可能性があります。 • [C6 state][C6_state] : CPU のアイドル時に、システムはC3 オプションの場合よりもさらに電力消費を減らします。このオプションでは、節約される電力が C0 または C2 よりも多くなりますが、サーバがフルパワーに戻るまで、パフォーマンス上の問題が発生する可能性があります。 • [C7 state][C7_state] : CPU のアイドル時に、サーバはコンポーネントが使用できる電力量を最小にします。このオプションでは、節約される電力量が最大になります。サーバがハイ パフォーマンス モードに戻るのに要する時間も最も長くなります。 • [No Limit][No_Limit] : サーバは、使用可能な任意の Cステートに入ることがあります。 <p>(注) このオプションは [CPU C State] がイネーブルの場合にのみ使用されます。</p>
[Patrol Scrub]	<p>システムがサーバ上のメモリの未使用部分でも単一ビットメモリ エラーをアクティブに探して訂正するかどうか。次のいずれかになります。</p> <ul style="list-style-type: none"> • [Disabled] : CPU がメモリ アドレスの読み取りまたは書き込みを行うときのみ、システムはメモリの ECC エラーをチェックします。 • [Enabled] : システムは定期的にメモリを読み書きして ECC エラーを探します。エラーが見つかったら、システムは修正を試みます。このオプションにより、単一ビットエラーは複数ビットエラーになる前に修正される場合がありますが、パトロールスクラブの実行時にパフォーマンスが低下する場合があります。

名前	説明
[Demand Scrub]	<p>システムがオンデマンドでのメモリのスクラビング処理を許可するかどうか。次のいずれかになります。</p> <ul style="list-style-type: none"> • [Disabled] : システムはオンデマンドでのメモリのスクラビング処理を許可しません。 • [Enabled] : システムはオンデマンドでのメモリのスクラビング処理を許可します。エラーが発生した場合、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。このプロセスは、システムを少数のデータ処理エラーにより迅速に実行します。
[Device Tagging]	<p>システムが、説明、アドレス、名前を含むさまざまな情報に基づいた、デバイスとインターフェイスのグループ化を許可するかどうか。次のいずれかになります。</p> <ul style="list-style-type: none"> • [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] : 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す。

詳細 : シリアルポート BIOS 設定

名前	説明
[Serial A Enable]	<p>シリアルポート A がイネーブルかディセーブルか。次のいずれかになります。</p> <ul style="list-style-type: none"> • [Disabled] : シリアルポートはディセーブルになります。 • [Enabled] : シリアルポートはイネーブルになります。

詳細 : USB BIOS 設定

名前	説明
[USB Port 0]	<p>プロセッサで USB ポート 0 を使用するかどうか。次のいずれかになります。</p> <ul style="list-style-type: none"> • [Disabled] : サーバで USB ポート 0 を使用しません。 • [Enabled] : プロセッサで USB ポート 0 を使用します。

名前	説明
[USB Port 1]	<p>プロセッサで USB ポート 1 を使用するかどうか。次のいずれかになります。</p> <ul style="list-style-type: none"> • [Disabled] : サーバで USB ポート 1 を使用しません。 • [Enabled] : プロセッサで USB ポート 1 を使用します。

サーバ管理 BIOS 設定

名前	説明
<p>[Reboot Host Immediately]</p> <p>NIM E シリーズ NCE には表示されません。</p>	<p>オンにすると、[Save Changes] をクリックした後ただちにサーバがリブートされます。</p> <p>サーバが自動ではリブートしないように指定するには、このチェックボックスをオフにします。パラメータの変更は、サーバが次にリブートされたときに有効になります。</p>
[Assert NMI on SERR]	<p>システムエラー (SERR) の発生時に、BIOS がマスク不能割り込み (NMI) を生成し、エラーをログに記録するかどうか。次のいずれかになります。</p> <ul style="list-style-type: none"> • [Disabled] : SERR の発生時に、BIOS は NMI を生成することもエラーをログに記録することもしません。 • [Enabled] : SERR の発生時に、BIOS は NMI を生成し、エラーをログに記録します。[Assert NMI on PERR] をイネーブルにする場合は、この設定をイネーブルにする必要があります。
[Assert NMI on PERR]	<p>プロセッサバスパリティエラー (PERR) の発生時に、BIOS がマスク不能割り込み (NMI) を生成し、エラーをログに記録するかどうか。次のいずれかになります。</p> <ul style="list-style-type: none"> • [Disabled] : PERR の発生時に、BIOS は NMI を生成することもエラーをログに記録することもしません。 • [Enabled] : PERR の発生時に、BIOS は NMI を生成し、エラーをログに記録します。この設定を使用するには、[Assert NMI on SERR] をイネーブルにする必要があります。

名前	説明
[FRB2 Enable]	<p>POST 中にシステムがハングした場合に、システムを回復するために CIMC によって FRB2 タイマーが使用されるかどうか。次のいずれかになります。</p> <ul style="list-style-type: none"> • [Disabled] : FRB2 タイマーは使用されません。 • [Enabled] : POST 中に FRB2 タイマーが開始され、必要に応じてシステムの回復に使用されます。
[Console Redirection]	<p>POST および BIOS のブート中に、シリアルポートをコンソールリダイレクションに使用できるようにします。BIOS のブートが完了し、オペレーティングシステムがサーバを担当すると、コンソールリダイレクションは関連がなくなり、無効になります。次のいずれかになります。</p> <ul style="list-style-type: none"> • [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][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。 [Serial Port A] オプションを選択する場合は、[Advanced] メニューの [Serial Port A] もイネーブルにする必要があります。 <p>(注) このオプションをイネーブルにする場合は、POST 中に表示される Quiet Boot のロゴ画面もディセーブルにします。</p>
[Flow Control]	<p>フロー制御にハンドシェイクプロトコルを使用するかどうか。送信要求/クリア ツー センド (RTS/CTS) は、隠れ端末の問題によって生じる可能性のあるフレーム衝突を減らすのに役立ちます。次のいずれかになります。</p> <ul style="list-style-type: none"> • [None] : フロー制御は使用されません。 • [RTS-CTS] : RTS/CTS がフロー制御に使用されます。 <p>(注) この設定は、リモート ターミナルアプリケーション上の設定と一致している必要があります。</p>

名前	説明
[Baud Rate]	<p>シリアルポートの伝送速度として使用されるボーレート。[Console Redirection]をディセーブルにした場合は、このオプションを使用できません。次のいずれかになります。</p> <ul style="list-style-type: none"> • [9.6k] : 9600 ボーレートが使用されます。 • [19.2k] : 19200 ボーレートが使用されます。 • [38.4k] : 38400 ボーレートが使用されます。 • [57.6k] : 57600 ボーレートが使用されます。 • [115.2k] : 115200 ボーレートが使用されます。 <p>(注) この設定は、リモートターミナルアプリケーション上の設定と一致している必要があります。</p>
[Terminal Type]	<p>コンソールリダイレクションに使用される文字フォーマットのタイプ。次のいずれかになります。</p> <ul style="list-style-type: none"> • [PC-ANSI] : PC-ANSI 端末フォントが使用されます。 • [VT100] : サポートされている vt100 ビデオ端末とその文字セットが使用されます。 • [VT100-PLUS] : サポートされている vt100-plus ビデオ端末とその文字セットが使用されます。 • [VT-UTF8] : UTF-8 文字セットのビデオ端末が使用されます。 <p>(注) この設定は、リモートターミナルアプリケーション上の設定と一致している必要があります。</p>

名前	説明
[OS Boot Watchdog Timer]	<p>BIOS が指定されたタイムアウト値でウォッチドッグ タイマーをプログラムするかどうか。タイマーが切れる前にオペレーティング システムのブートを完了しない場合、CIMC はシステムをリセットし、エラーがログに記録されます。次のいずれかになります。</p> <ul style="list-style-type: none"> • [Disabled] : サーバのブートにかかる時間をトラッキングするためにウォッチドッグタイマーは使用されません。 • [Enabled] : サーバのブートにかかる時間をウォッチドッグタイマーでトラッキングします。サーバが [OS Boot Watchdog Timer Timeout] フィールドに指定された時間内にブートしない場合、CIMC はエラーをログに記録し、[OS Boot Watchdog Policy] フィールドに指定されたアクションを実行します。 set OSBootWatchdogTimerTimeout コマンドで指定された時間内にブートしない場合、CIMC はエラーをログに記録し、 set OSBootWatchdogTimerPolicy コマンドで指定されたアクションを実行します。
[OS Boot Watchdog Timer Policy]	<p>ウォッチドッグタイマーが切れたときにシステムで実行されるアクション。次のいずれかになります。</p> <ul style="list-style-type: none"> • [Do Nothing] : OS のブート中にウォッチドッグタイマーが切れたときに、サーバの電源状態は変化しません。 • [Power Down] : OS のブート中にウォッチドッグタイマーが切れた場合、サーバの電源はオフになります。 • [Reset] : OS のブート中にウォッチドッグタイマーが切れた場合、サーバはリセットされます。 <p>(注) このオプションは [OS Boot Watchdog Timer] をイネーブルにした場合にのみ適用されます。</p>

共通コントロール

次の表に説明されているボタンは、[Configure BIOS Parameters] のすべてのタブで使用できます。

名前	説明
[Save Changes] ボタン	3つのタブすべてで、BIOS パラメータの設定を保存し、ウィザードを閉じます。 [Reboot Host Immediately] チェックボックスがオフの場合、サーバはすぐにリブートされ、新しいBIOS設定が有効になります。それ以外の場合は、サーバが手動でリブートされるまで変更は保存されます。
[Reset Values] ボタン	3つのタブすべての BIOS パラメータの値を、このダイアログボックスが開いたときに有効であった設定に戻します。
[Restore Defaults] ボタン	3つのタブすべての BIOS パラメータをそのデフォルト値に設定します。
[Cancel] ボタン	変更を行わずにダイアログボックスを閉じます。

トラステッドプラットフォーム モジュールの設定

トラステッドプラットフォームモジュール (TPM) は、サーバの認証に使用するアーティファクトを安全に保存できるコンポーネントです。これらのアーティファクトには、パスワード、証明書、または暗号キーを収録できます。プラットフォームが信頼性を維持していることを確認するうえで効果的なプラットフォームの尺度の保存でも、TPMを使用できます。すべての環境で安全なコンピューティングを実現するうえで、認証（プラットフォームがその表明どおりのものであることを証明すること）および立証（プラットフォームが信頼でき、セキュリティを維持していることを証明するプロセス）は必須の手順です。これは Intel の Trusted Execution Technology (TXT) セキュリティ機能の要件であり、TPM を搭載したサーバの BIOS 設定でイネーブルにする必要があります。デフォルトでは、TPM はこれらのサーバで有効になっています。

TPM の状態を確認するには、次の手順を実行します。

手順

-
- ステップ 1 システムの電源を入れます。
 - ステップ 2 最初のロゴ画面が表示されたらすぐに、**F2** キーまたは **DEL** キー（デスクトップがある場合）を押して、**BIOS** に移行します。
 - ステップ 3 **BIOS** のメニューで [Advanced] オプションに移動し、[Trusted Computing] ページを選択します。TPM 情報が表示されます。
-



第 4 章

RAID を使用したストレージの管理



(注) RAID 機能は E シリーズ サーバ および SME シリーズ NCE に適用されます。RAID 機能は EHWIC E シリーズ NCE および NIM E シリーズ NCE には適用されません。

この章は、次の項で構成されています。

- [RAID オプション, 52 ページ](#)
- [RAID の設定, 55 ページ](#)
- [RAID 設定の変更, 58 ページ](#)
- [RAID 設定の削除, 59 ページ](#)
- [物理ドライブの状態の変更, 60 ページ](#)
- [物理ドライブの再構築, 61 ページ](#)
- [物理ドライブの内容のクリア, 62 ページ](#)
- [ストレージコントローラ上での自動再構築のイネーブル化, 62 ページ](#)
- [仮想ドライブの削除, 63 ページ](#)
- [仮想ドライブの整合性検査の実行, 64 ページ](#)
- [仮想ドライブの再構築のオプション, 64 ページ](#)
- [ブート可能な仮想ドライブまたは物理ドライブの作成, 68 ページ](#)
- [2 TB を超える RAID ボリュームをサポートするための W2K12 のインストール, 70 ページ](#)

RAID オプション



(注) RAID機能はEシリーズサーバおよびSMEシリーズNCEに適用されます。RAID機能はEHWIC EシリーズNCEおよびNIM EシリーズNCEには適用されません。

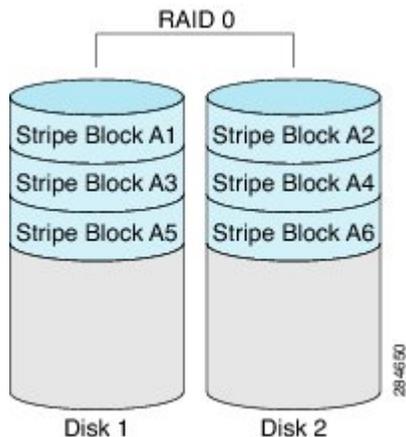
Eシリーズサーバのデータファイルは、ローカルの Redundant Array of Inexpensive Disks (RAID) に保存することもできます。次の RAID レベルがサポートされています。

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

RAID 0

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

図 5: RAID 0



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

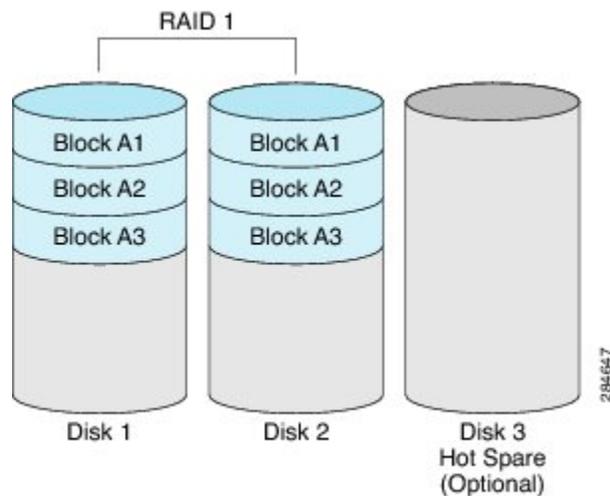
ただし、耐障害性、エラーチェック、ホットスペア、ホットスワップはありません。一方のディスク ドライブで障害が発生した場合は、アレイ全体のデータが破壊されます。エラーチェックやホットスワップの機能がないため、アレイは回復不能なエラーの影響を受けやすくなります。

RAID 1

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

図 6 : RAID 1



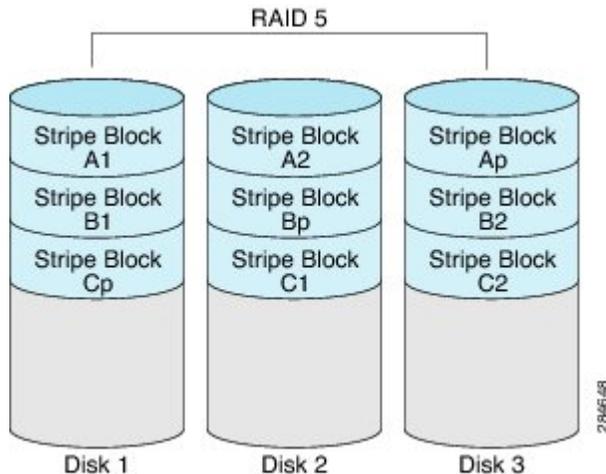
RAID 1 では、耐障害性とホットスワップがサポートされます。1 台のディスク ドライブで障害が発生した場合は、障害のあるディスク ドライブを取り外して新しいディスク ドライブに交換することができます。

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

RAID 5

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

図 7: RAID 5



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

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 モードでは、耐障害性、エラー チェック、ホットスワップ、ホットスペア、冗長性はサポートされません。

RAID オプションの概要

RAID オプション	説明	利点	欠点
RAID 0	冗長性なしでストライプブロックに均等に保存されるデータ	<ul style="list-style-type: none"> 優れたストレージ効率 パフォーマンスの向上 	<ul style="list-style-type: none"> エラー チェックなし 耐障害性なし ホットスワップなし 冗長性なし ホットスペアなし

RAID 1	ディスクドライブのミラーセットとオプションのホットスペアディスクドライブ	<ul style="list-style-type: none"> • 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 	<ul style="list-style-type: none"> • ストレージの減少 • パフォーマンス上の影響
RAID 5	すべてのディスクドライブにわたってストライプブロックに保存されるデータと分散されたパリティデータ	<ul style="list-style-type: none"> • RAID 1 よりも優れたストレージ効率 • RAID 0 よりも優れた耐障害性 • 低コストの冗長性 • ホットスワップ 	<ul style="list-style-type: none"> • 低いパフォーマンス
非 RAID	RAID が設定されていないディスクドライブ JBOD と呼ばれます	<ul style="list-style-type: none"> • ポータブル 	<ul style="list-style-type: none"> • 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



(注) RAID 機能は E シリーズサーバおよび SME シリーズ NCE に適用されます。RAID 機能は EHWIC E シリーズ NCE および NIM E シリーズ NCE には適用されません。

仮想ドライブの RAID レベル、ストリップサイズ、ホストアクセス権限、ドライブキャッシング、および初期化パラメータを設定するには、次の手順を実行します。この手順を使用して、ドライブをホットスペアドライブに指定したり、ドライブをブート可能にしたりすることもできます。

手順

- ステップ 1** [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2** [Server] タブの [RAID] をクリックします。次のいずれかを実行します。
- [Configure Virtual Drive] ダイアログ ボックスが表示されない場合は、次の手順に進みます。
 - [Configure Virtual Drive] ダイアログ ボックスが表示され、仮想ドライブが設定されていない場合は、ステップ 5 に示すようにフィールドを入力します。
- ステップ 3** [Storage Card] 領域のタブ メニューで、[Virtual Drive Info] タブをクリックします。
- ステップ 4** [Virtual Drive Info] タブの [Actions] 領域で、[Create] をクリックします。
- ステップ 5** 必要に応じて次のフィールドに値を入力します。

名前	説明
[Available Drives] テーブル	RAID 設定で使用できるドライブを表示します。 (注) ドライブを移動するには、ドライブをクリックして適切なテーブルにドラッグします。
[Selected Drives] テーブル	RAID 設定に選択されたドライブを表示します。 (注) ドライブを移動するには、ドライブをクリックして適切なテーブルにドラッグします。
[RAID Level] ドロップダウンリスト	RAID レベルのオプション。次のいずれかになります。 <ul style="list-style-type: none"> • [RAID 0] : ブロック ストライピング。 • [RAID 1] : ミラーリング。 • [RAID 5] : パリティを使用したブロック ストライピング。 (注) シングル幅の E シリーズ サーバでは、RAID 0 および RAID 1 レベルがサポートされます。ダブル幅の E シリーズ サーバでは、RAID 0、RAID 1、および RAID 5 レベルがサポートされます。PCIe オプションを搭載したダブル幅の 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。
[Name] フィールド	仮想ドライブの名前。 最大 15 文字を入力します。数字、大文字、および小文字を使用できます。特殊文字はサポートされていません。

名前	説明
[Strip Size] ドロップダウンリスト	<p>ストリップ サイズのオプション。次のいずれかになります。</p> <ul style="list-style-type: none"> • 64 KB • 32KB • 16 KB • 8 KB
[Initialization] ドロップダウンリスト	<p>コントローラによるドライブの初期化方法。次のいずれかになります。</p> <ul style="list-style-type: none"> • [Quick] : コントローラはただちにドライブを初期設定します。これがデフォルトであり、推奨オプションです。 • [Full] : コントローラは新しい設定を完全に初期化します。 <ul style="list-style-type: none"> (注) ドライブのサイズによっては、[Full] 初期化は完了するまで数時間かかる場合があります。進行状況を確認するには、[General] 領域の [Initialize Progress] フィールドと [Initialize Time Elapsed] フィールドを参照します。 • [None] : コントローラはドライブを初期化しません。
[Drive Cache] ドロップダウンリスト	<p>コントローラによるドライブキャッシングの処理方法。次のいずれかになります。</p> <ul style="list-style-type: none"> • [Disable] : ドライブでのキャッシングはディセーブルになります。 <ul style="list-style-type: none"> (注) これがデフォルトであり、推奨オプションです。 • [Unchanged] : コントローラでは、ドライブで指定されたキャッシングポリシーを使用します。これがデフォルトであり、推奨オプションです。 • [Enable] : ドライブでのキャッシングはイネーブルになります。このオプションは、データへのアクセス遅延を最小限に抑えます。 <ul style="list-style-type: none"> 注意 ドライブのキャッシュをイネーブルにすると、ハードディスクドライブに対するすべての保証が無効になります。この設定オプションはサポートされていません。このオプションは、自己の責任において使用してください。

名前	説明
[Access Policy] ドロップダウンリスト	ホストのアクセス権限を設定します。次のいずれかになります。 <ul style="list-style-type: none"> • [Read-Write] : ホストはドライブにフルアクセスできます。 • [Read Only] : ホストはドライブからデータの読み取りだけを実行できます。 • [Blocked] : ホストはドライブにアクセスできません。
[Set this Virtual Drive Bootable] チェックボックス	コントローラによるドライブのブート方法。次のいずれかになります。 <ul style="list-style-type: none"> • [Enable] : コントローラはこのドライブをブート可能にします。 • [Disable] : このドライブはブートできません。 <p>(注) オペレーティング システムまたはハイパーバイザを RAID アレイにインストールする場合は、このチェックボックスをオンにすることをお勧めします。</p>
[Use the Remaining Drive as Hot Spare] チェックボックス	[Available Drives] テーブル内のドライブをホットスペアドライブとして指定します。 <p>(注) RAID 1 にのみ適用できます。このチェックボックスは、他の RAID レベルではグレーアウトされます。ダブル幅の E シリーズ サーバに適用可能。</p>

ステップ 6 RAID 設定を確認し、[Confirm] をクリックして変更を確定します。

RAID 設定の変更



(注) RAID 機能は E シリーズ サーバおよび SME シリーズ NCE に適用されます。RAID 機能は EHWIC E シリーズ NCE および NIM E シリーズ NCE には適用されません。

この手順を使用して、ストレージコントローラの自動再構築を有効または無効にします。

手順

- ステップ 1** [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2** [Server] タブの [RAID] をクリックします。
- ステップ 3** [Storage Card] 領域のタブ メニューで、[Virtual Drive Info] タブをクリックします。
- ステップ 4** [Virtual Drive Info] タブの [Actions] 領域で、[Edit] をクリックします。
[Modify RAID Configuration] ダイアログボックスが表示されます。必要に応じて次のフィールドを変更します。

名前	説明
[Enable Auto Rebuild] または [Disable Auto Rebuild] ボタン	<p>仮想ドライブが劣化したときに、新しいドライブ上で再構築プロセスを自動的に開始するかどうかを示します。次のいずれかになります。</p> <ul style="list-style-type: none"> • [Enabled] : ドライブが劣化し、新しいドライブが差し込まれた場合、新しいドライブで再構築プロセスが自動的に開始されます。 <p>(注) 再構築プロセスでは、既存のすべてのデータが上書きされます。そのため、接続するドライブに重要なデータが格納されていないことを確認してください。</p> <ul style="list-style-type: none"> • [Disabled] : ドライブが劣化し、新しいドライブが差し込まれた場合、新しいドライブが無視されます。新しいドライブで再構築プロセスを手動で開始する必要があります。 <p>重要 [Disable Auto Rebuild] ボタンが表示されている場合、自動再構築が有効であることを示します。</p>

RAID 設定の削除



- (注) RAID 機能は E シリーズサーバおよび SME シリーズ NCE に適用されます。RAID 機能は EHWIC E シリーズ NCE および NIM E シリーズ NCE には適用されません。

すべての RAID 設定または外部設定をクリアするには、次の手順を実行します。

手順

- ステップ 1 [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2 [Server] タブの [RAID] をクリックします。
- ステップ 3 [Storage Card] 領域のタブメニューで、[Virtual Drive Info] タブをクリックします。
- ステップ 4 [Virtual Drive Info] タブの [Actions] 領域で、[Delete] をクリックします。
[Clear Configurations] ダイアログボックスが表示されます。必要に応じて次を実行します。

名前	説明
[Clear All RAID Config] オプション ボタン	すべての RAID 設定を削除します。 注意 このオプション ボタンをクリックすると、ドライブ内の既存データがすべて削除されます。
[Clear Foreign Config] オプション ボタン	すべての外部設定を削除します。 別の E シリーズサーバからドライブを差し込む場合、そのドライブを使用可能にするには外部設定をクリアする必要があります。 (注) このオプション ボタンをクリックすると、新しく差し込まれたドライブ内の設定のみ削除され、既存ドライブ内の設定は変更されません。
[Proceed] ボタン	削除操作を続行します。

物理ドライブの状態の変更



- (注) RAID機能はEシリーズサーバおよびSMEシリーズNCEに適用されます。RAID機能はEHWIC EシリーズNCEおよびNIM EシリーズNCEには適用されません。

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

-
- ステップ 1** [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2** [Server] タブの [RAID] をクリックします。
- ステップ 3** [Storage Card] 領域のタブ メニューで、[Physical Drive Info] タブをクリックします。
- ステップ 4** [Physical Drives] ペインの [Actions] カラムで、[Change State To] リストから次のいずれかを選択します。
- [hotspare] : ドライブをスペア ドライブに指定します。
 - [jbd] : ドライブを RAID として設定しません。
 - [unconfigured good] : ドライブをドライブ グループまたはホット スペア プールに割り当てる
ことができます。
- ステップ 5** [OK] をクリックして確定します。
-

物理ドライブの再構築



- (注) RAID 機能は E シリーズサーバおよび SME シリーズ NCE に適用されます。RAID 機能は EHWIC E シリーズ NCE および NIM E シリーズ NCE には適用されません。

物理ドライブ上で再構築プロセスを手動で開始するには、次の手順を実行します。

手順

-
- ステップ 1** [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2** [Server] タブの [RAID] をクリックします。
- ステップ 3** [Storage Card] 領域のタブ メニューで、[Physical Drive Info] タブをクリックします。
- ステップ 4** [Physical Drives] ペインの [Actions] カラムで、ドロップダウンリストから [Rebuild] を選択し、[OK] をクリックして確定します。
再構築プロセスは、完了までに数時間かかります。
- (注) 物理ドライブの状態が [Failed] または [Offline] の場合、ドロップダウンリストに [Rebuild] オプションが表示されます。

- ステップ 5 再構築プロセスの進行状況を確認する場合は、[General] 領域の [Rebuilding Progress] フィールドと [Rebuilding Time Elapsed] フィールドを参照します。
- ステップ 6 再構築プロセスを停止する場合は、[General] 領域の [Rebuilding Progress] フィールドの横にある [Abort] ボタンをクリックし、[OK] をクリックして確定します。

物理ドライブの内容のクリア



(注) RAID機能はEシリーズサーバおよびSMEシリーズNCEに適用されます。RAID機能はEHWIC EシリーズNCEおよびNIM EシリーズNCEには適用されません。

物理ドライブの内容をすべて消去して、ゼロに設定するには、次の手順を使用します。

手順

- ステップ 1 [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2 [Server] タブの [RAID] をクリックします。
- ステップ 3 [Storage Card] 領域のタブメニューで、[Physical Drive Info] タブをクリックします。
- ステップ 4 [Physical Drives] ペインの [Actions] カラムで、ドロップダウンリストから [Erase] を選択し、[OK] をクリックして確定します。
消去プロセスは、完了までに数時間かかります。
- ステップ 5 消去プロセスの進行状況を確認する場合は、[General] 領域の [Erasing Progress] フィールドと [Erasing Time Elapsed] フィールドを参照します。
- ステップ 6 消去プロセスを停止する場合は、[General] 領域の [Erasing Progress] フィールドの横にある [Abort] ボタンをクリックし、[OK] をクリックして確定します。

ストレージコントローラ上での自動再構築のイネーブル化



(注) RAID機能はEシリーズサーバおよびSMEシリーズNCEに適用されます。RAID機能はEHWIC EシリーズNCEおよびNIM EシリーズNCEには適用されません。

ディスク ドライブを自動的に再構築するには、次の手順を実行します。RAID 構成内のいずれかのディスク ドライブが劣化し、新しいドライブが接続されると、新しいドライブで再構築プロセスが自動的に開始されます。

手順

-
- ステップ 1** [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2** [Server] タブの [RAID] をクリックします。
- ステップ 3** [Storage Adapters] 領域で、ストレージカードを選択します。
サーバの電源がオンになっている場合、選択したストレージアダプタのリソースが [Storage Card] 領域のタブ メニューに表示されます。
- ステップ 4** [Storage Card] 領域のタブ メニューで、[Virtual Drive Info] タブをクリックします。
- ステップ 5** [Virtual Drive Info] タブの [Actions] 領域で、[Edit] をクリックします。
[Modify RAID Configuration] ダイアログボックスが表示されます。
- ステップ 6** [Enable Auto Rebuild] ボタンが表示されている場合は、このボタンをクリックして、[Disable Auto Rebuild] ボタンを表示します。
[Disable Auto Rebuild] ボタンが表示されている場合、自動再構築が有効であることを示します。
- 注意** 再構築プロセスでは、既存のすべてのデータが上書きされます。そのため、接続するドライブに重要なデータが格納されていないことを確認してください。
-

仮想ドライブの削除



- (注) RAID 機能はEシリーズサーバおよびSMEシリーズNCEに適用されます。RAID 機能はEHWIC EシリーズNCEおよびNIM EシリーズNCEには適用されません。
-

手順

-
- ステップ 1** [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2** [Server] タブの [RAID] をクリックします。
- ステップ 3** [Storage Card] 領域のタブ メニューで、[Virtual Drive Info] タブをクリックします。
- ステップ 4** [Virtual Drives] 領域の [Actions] カラムで、[Delete] オプションを選択します。
- ステップ 5** [OK] をクリックして確定します。
-

仮想ドライブの整合性検査の実行



(注) RAID機能はEシリーズサーバおよびSMEシリーズNCEに適用されます。RAID機能はEHWIC EシリーズNCEおよびNIM EシリーズNCEには適用されません。

この手順を使用して、仮想ドライブの整合性検査を実行します。次のいずれかになります。

- RAID 1 : 両方のドライブのデータが同一かどうかを確認します。
- 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。

手順

- ステップ 1 [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2 [Server] タブの [RAID] をクリックします。
- ステップ 3 [Storage Card] 領域のタブメニューで、[Virtual Drive Info] タブをクリックします。
- ステップ 4 [Virtual Drives] 領域の [Actions] カラムで [Consistency Check] オプションを選択し、[OK] をクリックして確定します。
整合性検査プロセスは、完了までに数時間かかります。
- ステップ 5 整合性検査プロセスの進行状況を確認する場合は、[General] 領域の [Consistency Check Progress] フィールドと [Consistency Check Time Elapsed] フィールドを参照します。
- ステップ 6 整合性検査プロセスを停止する場合は、[General] 領域の [Consistency Check Progress] フィールドの横にある [Abort] ボタンをクリックし、[OK] をクリックして確定します。

仮想ドライブの再構築のオプション



(注) RAID機能はEシリーズサーバおよびSMEシリーズNCEに適用されます。RAID機能はEHWIC EシリーズNCEおよびNIM EシリーズNCEには適用されません。

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き、仮想ドライブのサイズは維持または増加されます。

仮想ドライブのサイズは維持または増加させることはできますが、減少させ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、同じ台数のドライブで RAID 1 に移行することはできません。これは、RAID 1 では、仮想ドライブのサイズを以前の半分に減らした、ミ

ラーリングされた一連のディスク ドライブが作成されるためです。これはサポートされていません。

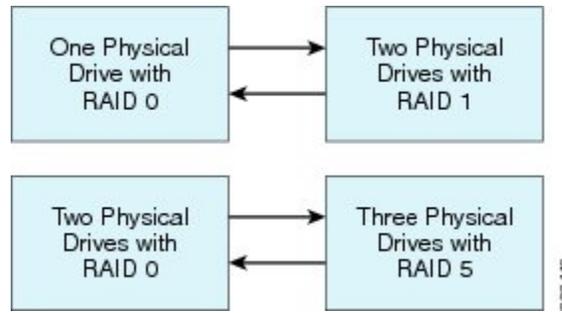


(注) 仮想ドライブの再構築プロセスは、完了までに数時間かかることがあります。再構築プロセス中も、システムを引き続き使用できます。

仮想ドライブのサイズを保持するオプション

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

図 8: 仮想ドライブ サイズが維持されるオプション



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

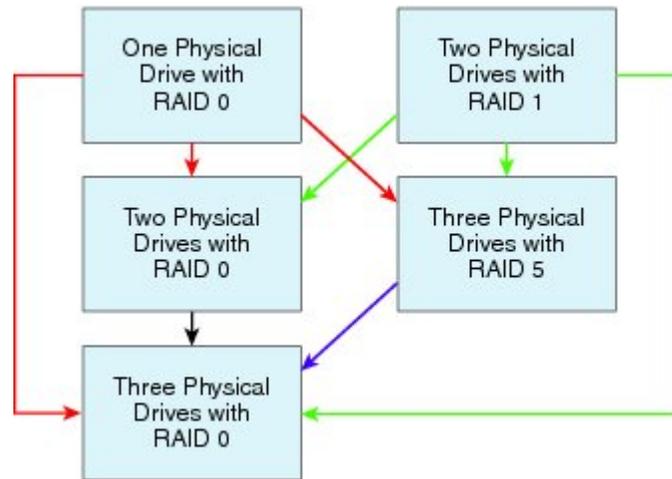
表 3: 仮想ドライブ サイズの維持

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

仮想ドライブのサイズを増やすためのオプション

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

図 9: 仮想ドライブサイズが増加するオプション



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

表 4: 仮想ドライブサイズの増加

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

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

仮想ドライブの再構築



(注) RAID 機能は E シリーズサーバおよび SME シリーズ NCE に適用されます。RAID 機能は EHWIC E シリーズ NCE および NIM E シリーズ NCE には適用されません。

仮想ドライブを新しい RAID レベルに移行（再構築）するには、次の手順を実行します。

はじめる前に

「[仮想ドライブの再構築のオプション](#)」を参照してください。

手順

- ステップ 1 [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2 [Server] タブの [RAID] をクリックします。
- ステップ 3 [Storage Card] 領域のタブメニューで、[Virtual Drive Info] タブをクリックします。
- ステップ 4 [Virtual Drives] 領域の [Actions] カラムで、[Reconstruct] オプションを選択します。
[Reconstruct Virtual Drive] ダイアログボックスが表示されます。
- ステップ 5 必要に応じて次のものに値を入力します。

名前	説明
[Migrate RAID Level] オプション ボタン	このオプションを選択し、指定された新しい RAID レベルに仮想ドライブを移行します。
[Add Drives] オプション ボタン	このオプションを選択し、追加するドライブを [Add from Available Drives] テーブルから選択します。
[Remove Drives] オプション ボタン	このオプションを選択し、削除するドライブを [Remove from Configured Drives] テーブルから選択します。

名前	説明
[Add from Available Drives] テーブル	新しい RAID レベルに移行するために追加できる物理ドライブが一覧表示されます。 (注) このテーブルは、[Add Drives] オプション ボタンを選択するとアクティブになります。
[Remove from Configured Drives] テーブル	新しい RAID レベルに移行するために削除できる物理ドライブが一覧表示されます。 (注) このテーブルは、[Remove Drives] オプション ボタンを選択するとアクティブになります。
[From Current Level: RAID x Migrate To:] ドロップダウンリスト	ドライブを移行する新しい RAID レベル。[Confirm] をクリックした後に、再構築プロセスを開始します。 (注) 仮想ドライブのサイズは維持または増加させることはできますが、減少させることはできません。

再構築プロセスは、完了までに数時間かかります。

- ステップ 6** 再構築プロセスの進行状況を確認する場合は、[General] 領域の [Reconstruct Progress] フィールドと [Reconstruct Time Elapsed] フィールドを参照します。

ブート可能な仮想ドライブまたは物理ドライブの作成



- (注) RAID 機能は E シリーズ サーバ および SME シリーズ NCE に適用されます。RAID 機能は EHWIC E シリーズ NCE および NIM E シリーズ NCE には適用されません。

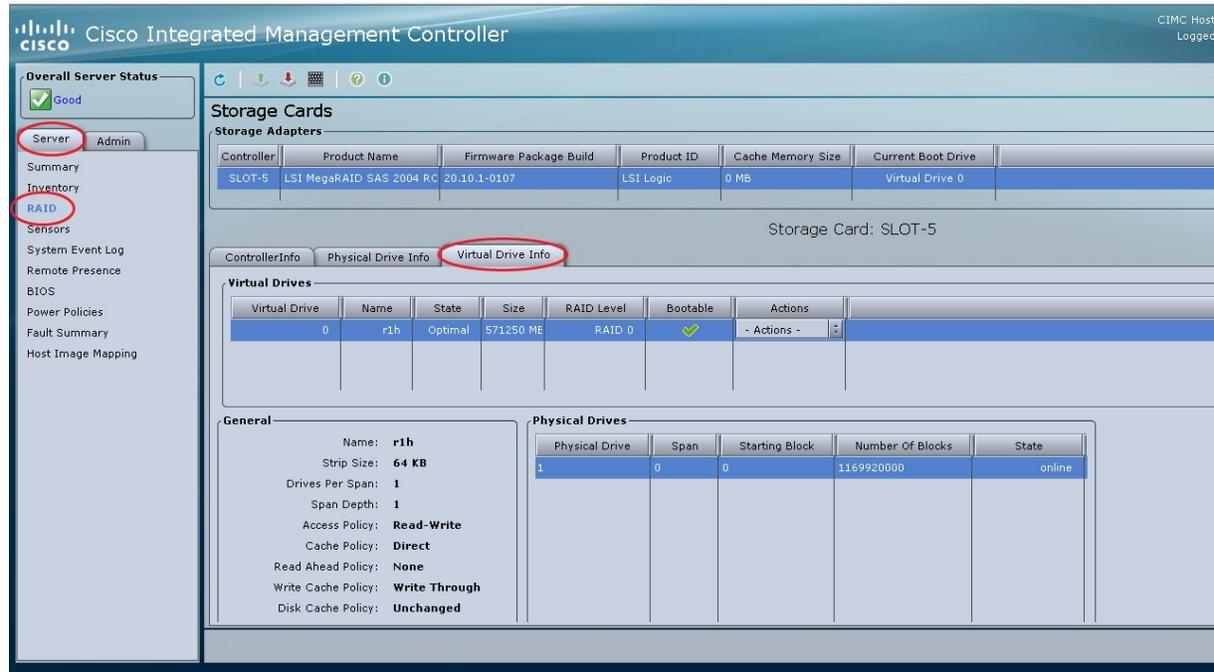
RAID を設定する場合、[Configure Virtual Drive] ダイアログボックスに、ディスク ドライブをブート可能にするチェックボックスがあります。RAID 設定プロセスで [Set this Virtual Drive Bootable] チェックボックスをオンにしなかった場合は、次の手順によりディスク ドライブをブート可能にできます。

手順

- ステップ 1** [Navigation] ペインの [Server] メニューをクリックします。
ステップ 2 [Server] タブの [RAID] をクリックします。
ステップ 3 仮想ドライブをブート可能にするには、次を実行します。

- a) [Storage Card] 領域のタブメニューで、[Virtual Drive Info] タブをクリックします。

図 10 : [Virtual Drive Info] タブ

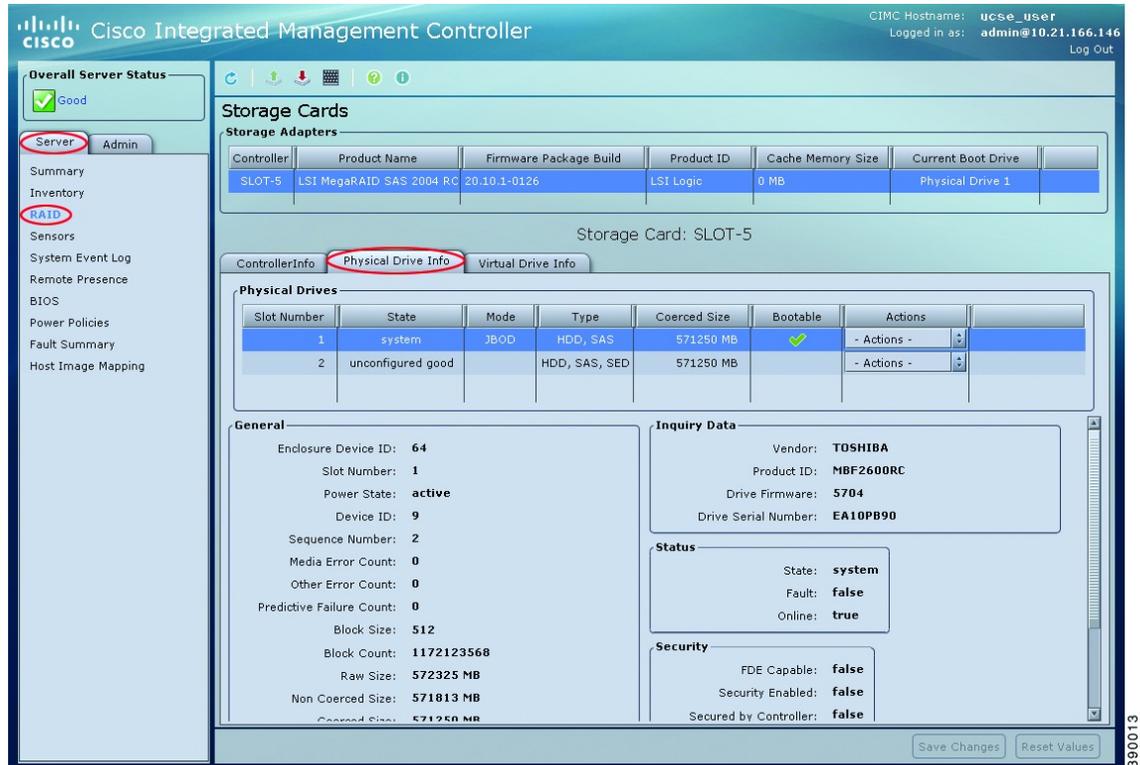


- b) 該当する仮想ドライブの [Actions] カラムにあるドロップダウンリストから、[Set Bootable] を選択します。
- c) [OK] をクリックして、ブートドライブをこの仮想ドライブに変更します。
 (注) ドライブをブート可能に設定すると、[Bootable] カラムに設定したドライブに対するチェックマークが表示されます。

ステップ 4 物理ドライブをブート可能にするには、次を実行します。

- a) [Storage Card] 領域のタブメニューで、[Physical Drive Info] タブをクリックします。

図 11 : [Physical Drive Info] タブ



- b) 該当する物理ドライブの [Actions] カラムにあるドロップダウンリストから、[Set Bootable] を選択します。
- c) [OK] をクリックして、ブート ドライブをこの物理ドライブに変更します。
 (注) 物理ドライブは、ブート可能にするには非 RAID モードである必要があります。ドライブをブート可能に設定すると、[Bootable] カラムに設定したドライブに対するチェックマークが表示されます。

2 TB を超える RAID ボリュームをサポートするための W2K12 のインストール

UCS-E160D-M2 シリーズサーバで、容量が 2 TB を超えるハードドライブを設置して Windows を実行する場合は、この項で説明されている手順に従ってください。W2K12 のインストール方法には、レガシー BIOS を使用する方法と UEFI を使用する方法があります。

2 TB を超える RAID ボリュームをサポートするための、レガシー BIOS を使用した W2K12 のインストール

この回避策では、2 TB を超える RAID ボリュームをサポートするための、レガシー BIOS を使用した W2K12 のインストール方法を示します。この回避策には、次の主要なタスクが含まれます。

- 1 すべてのドライブを「Unconfigured Good」状態に設定します。
- 2 最初のハードディスクを使用して仮想ドライブ 0 (VD0) を設定し、RAID 0 に配置します。W2K12 は VD0 にインストールされます。
- 3 残りのハードディスクを使用して仮想ドライブ 1 (VD1) を設定し、RAID 0 に配置します。W2K12 を使用してこのボリュームを GPT に変換して、ストレージ全体にアクセスできるようにします。

詳細な手順は次のとおりです。

手順

- ステップ 1 すべてのドライブを「Unconfigured Good」状態に設定します。参照 [物理ドライブの状態の変更](#) (60 ページ)
- ステップ 2 [Storage Card] 領域のタブメニューで、[Virtual Drive Info] タブをクリックします。

図 12 : [Virtual Drive Info] タブ

The screenshot shows the Cisco Integrated Management Controller (CIMC) GUI. The main content area is titled "Storage Cards" and "Storage Adapters". Below this, there is a table for "Storage Adapters" with columns: Controller, Product Name, Firmware Package Build, Product ID, Cache Memory Size, and Current Boot Drive. The table contains one entry for SLOT-5.

Below the adapters table, there is a section for "Storage Card: SLOT-5" with tabs for "Controller Info", "Physical Drive Info", and "Virtual Drive Info". The "Virtual Drive Info" tab is selected, showing a "Virtual Drives" table with columns: Virtual Drive, Name, State, Size, RAID Level, Bootable, and Actions. The table is currently empty.

Below the virtual drives table, there is a "General" section with various RAID configuration parameters and a "Physical Drives" table. The "Physical Drives" table has columns: Physical Drive, Span, Starting Block, Number Of Blocks, and State. It contains one entry for Physical Drive 1.

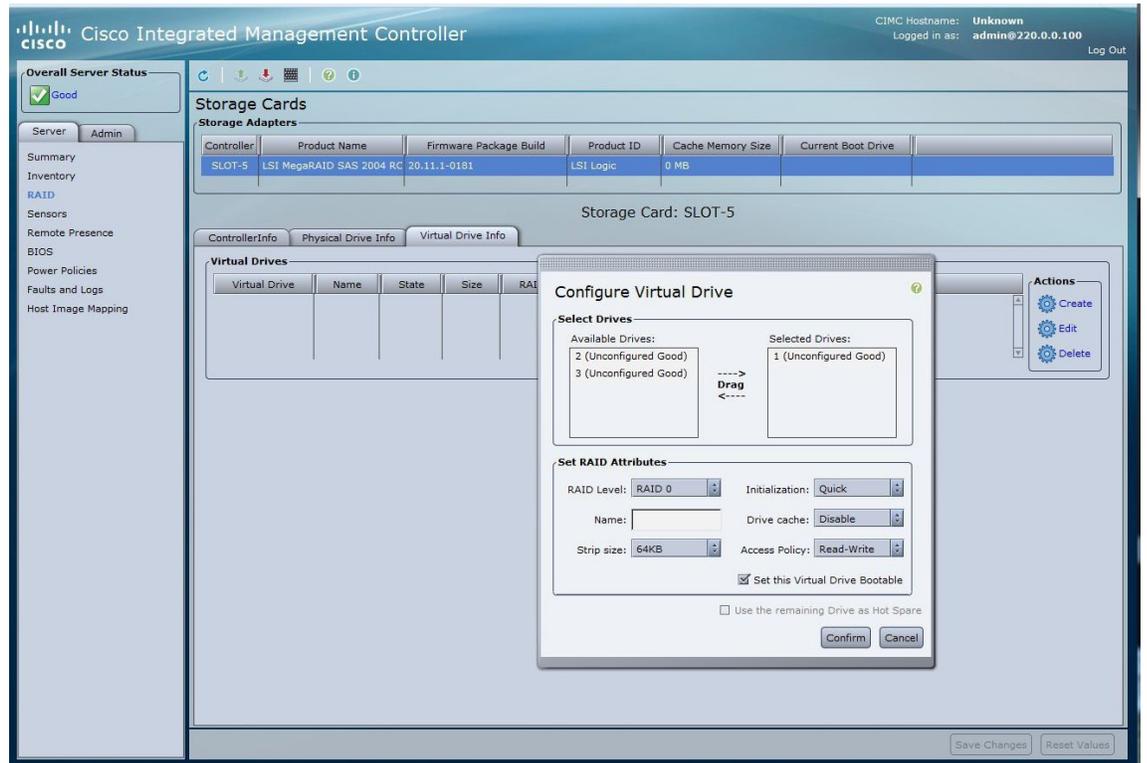
Controller	Product Name	Firmware Package Build	Product ID	Cache Memory Size	Current Boot Drive
SLOT-5	LSI MegaRAID SAS 2004 RC	20.11.1-0101	LSI Logic	0 MB	Virtual Drive 0

Virtual Drive	Name	State	Size	RAID Level	Bootable	Actions
---------------	------	-------	------	------------	----------	---------

Physical Drive	Span	Starting Block	Number Of Blocks	State
1	0	0	351508896	online

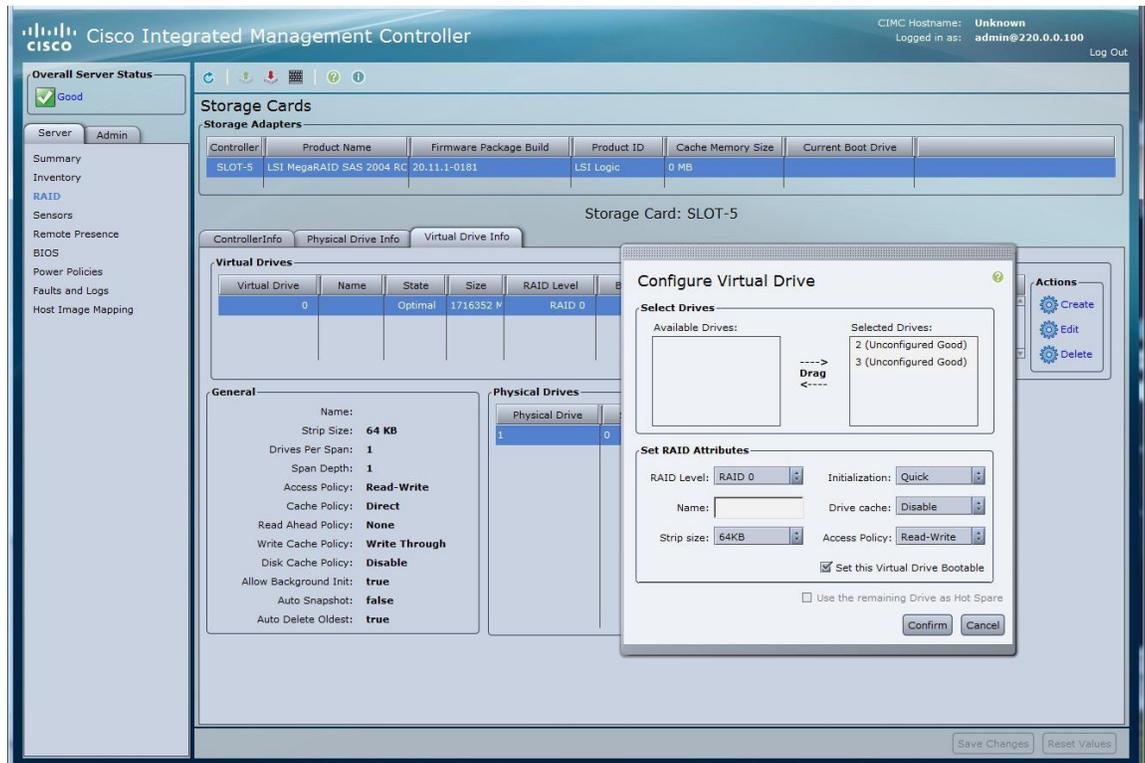
ステップ 3 [Virtual Drive Info] タブの [Actions] 領域で、[Create] をクリックします。[Configure Virtual Drive] ダイアログボックスが表示されます。

図 13: 仮想ドライブ 0 の設定



- ステップ 4 [Available Devices] からドライブ 1 を選択して [Selected Devices] にドラッグします。
- ステップ 5 [Confirm] をクリックします。仮想ドライブ 0 が作成されました。
- ステップ 6 [Virtual Drive Info] タブの [Actions] 領域で、[Create] をクリックします。[Configure Virtual Drive] ダイアログボックスが表示されます。
- ステップ 7 [Available Devices] から残りのドライブを選択して [Selected Devices] にドラッグします。

図 14: 仮想ドライブ 1 の設定



ステップ 8 [Confirm] をクリックします。仮想ドライブ 1 が作成されました。仮想ドライブを確認します。

図 15: 仮想ドライブの確認

Cisco Integrated Management Controller

CIMC Hostname: Unknown
Logged in as: admin@220.0.0.100
Log Out

Overall Server Status: **Good**

Server Admin

Summary
Inventory
RAID
Sensors
Remote Presence
BIOS
Power Policies
Faults and Logs
Host Image Mapping

Storage Cards

Storage Adapters

Controller	Product Name	Firmware Package Build	Product ID	Cache Memory Size	Current Boot Drive
SLOT-5	LSI MegaRAID SAS 2004 RC	20.11.1-0181	LSI Logic	0 MB	Virtual Drive 0

Storage Card: SLOT-5

Controller Info Physical Drive Info Virtual Drive Info

Virtual Drives

Virtual Drive	Name	State	Size	RAID Level	Bootable	Actions
0		Optimal	1716352 M	RAID 0	✓	- Actions -
1		Optimal	3432704 M	RAID 0		- Actions -

Actions: Create, Edit, Delete

General

Name:
Strip Size: **64 KB**
Drives Per Span: **1**
Span Depth: **1**
Access Policy: **Read-Write**
Cache Policy: **Direct**
Read Ahead Policy: **None**
Write Cache Policy: **Write Through**
Disk Cache Policy: **Disable**
Allow Background Init: **true**
Auto Snapshot: **false**
Auto Delete Oldest: **true**

Physical Drives

Physical Drive	Span	Starting Block	Number Of Blocks	State
1	0	0	3515088896	online

Save Changes Reset Values

ステップ 9 ホストイメージマッピングまたは vKVM を使用して、W2K12 を仮想ドライブ 0 にインストールします。

図 16: 仮想ドライブ 0 への W2K12 のインストール

The screenshot displays the Cisco Integrated Management Controller (CIMC) GUI. The main content area is titled "Storage Cards" and shows the configuration for a "Storage Card: SLOT-5".

Storage Adapters Table:

Controller	Product Name	Firmware Package Build	Product ID	Cache Memory Size	Current Boot Drive
SLOT-5	LSI MegaRAID SAS 2004 RC	20.11.1-0181	LSI Logic	0 MB	Virtual Drive 0

Virtual Drives Table:

Virtual Drive	Name	State	Size	RAID Level	Bootable	Actions
0		Optimal	1716352 M	RAID 0	✓	- Actions -
1		Optimal	3432704 M	RAID 0		- Actions -

General Configuration:

- Name:
- Strip Size: **64 KB**
- Drives Per Span: **1**
- Span Depth: **1**
- Access Policy: **Read-Write**
- Cache Policy: **Direct**
- Read Ahead Policy: **None**
- Write Cache Policy: **Write Through**
- Disk Cache Policy: **Disable**
- Allow Background Init: **true**
- Auto Snapshot: **false**
- Auto Delete Oldest: **true**

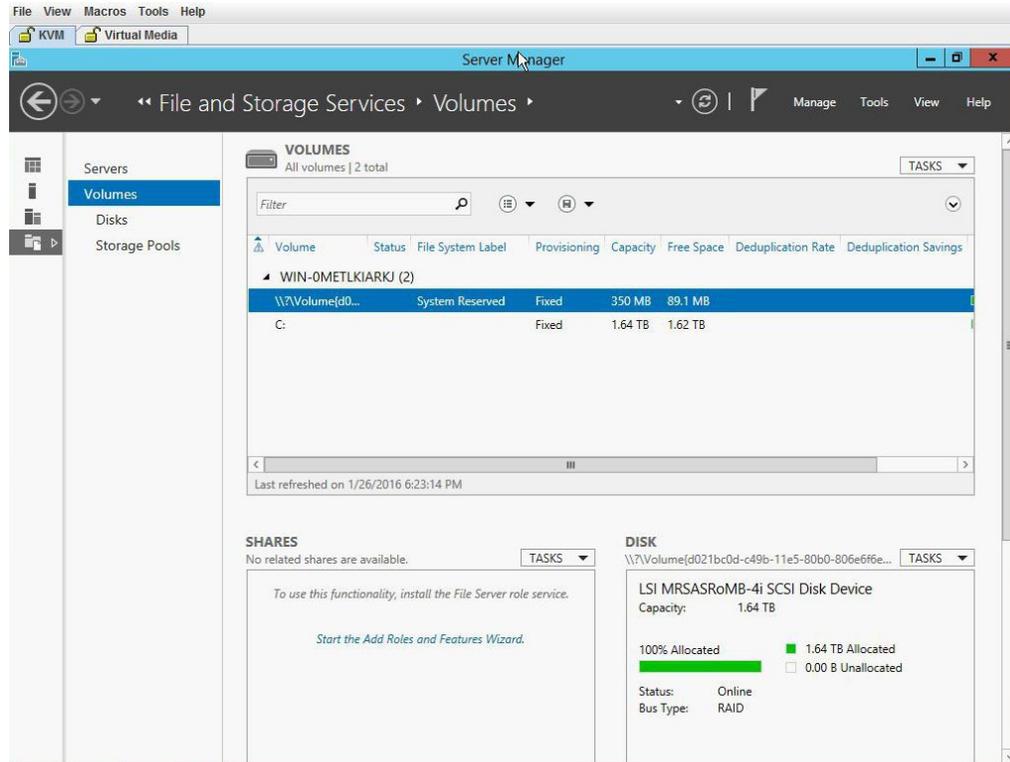
Physical Drives Table:

Physical Drive	Span	Starting Block	Number Of Blocks	State
1	0	0	351508896	online

The interface also shows "Overall Server Status" as "Good" and includes a "Save Changes" button at the bottom right.

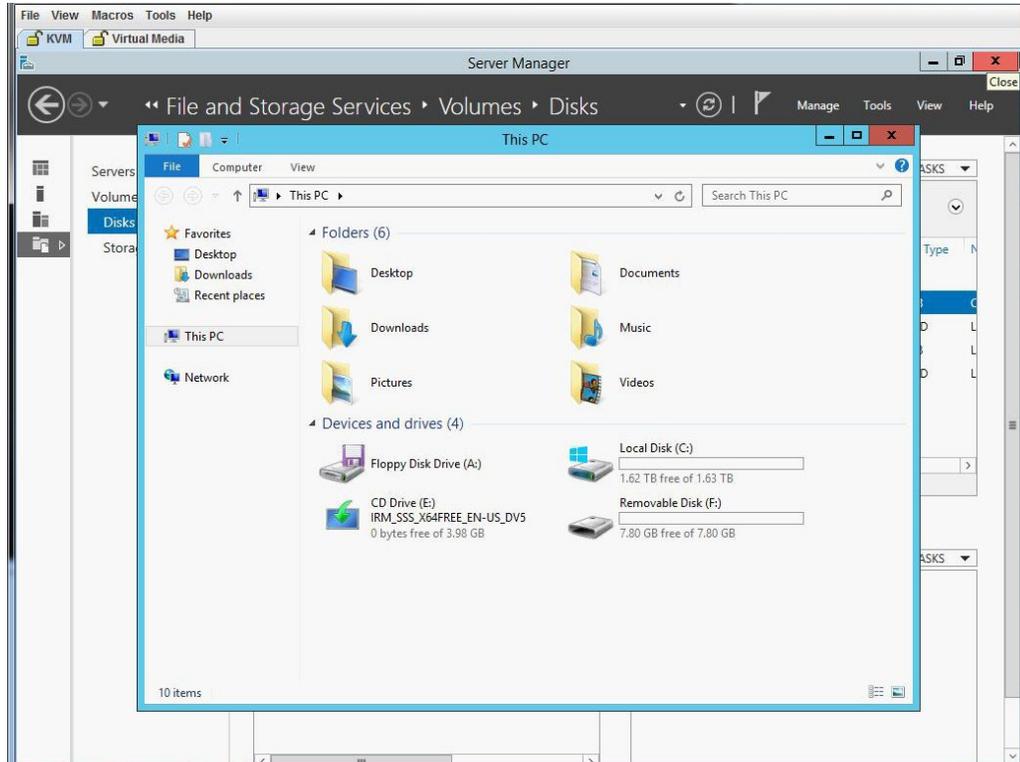
ステップ 10 W2K12 をインストールしたら、ログインして、ボリュームのステータスを確認します。

図 17: ボリュームのステータス



ステップ 11 C ドライブのストレージサイズを確認します。

図 18: C ドライブのストレージサイズ



ステップ 12 [Disk] に移動し、仮想ドライブ 1 を使用して新しいボリュームを作成します。仮想ドライブ 1 を選択して右クリックします。[New Volume] をクリックします。[New Volume] ウィザードが表示さ

れます。このウィザードでは、ボリュームの作成、ボリュームのドライブ文字の割り当て、ファイルシステムを指定したボリュームのフォーマットができます。

図 19：新規ボリュームの作成

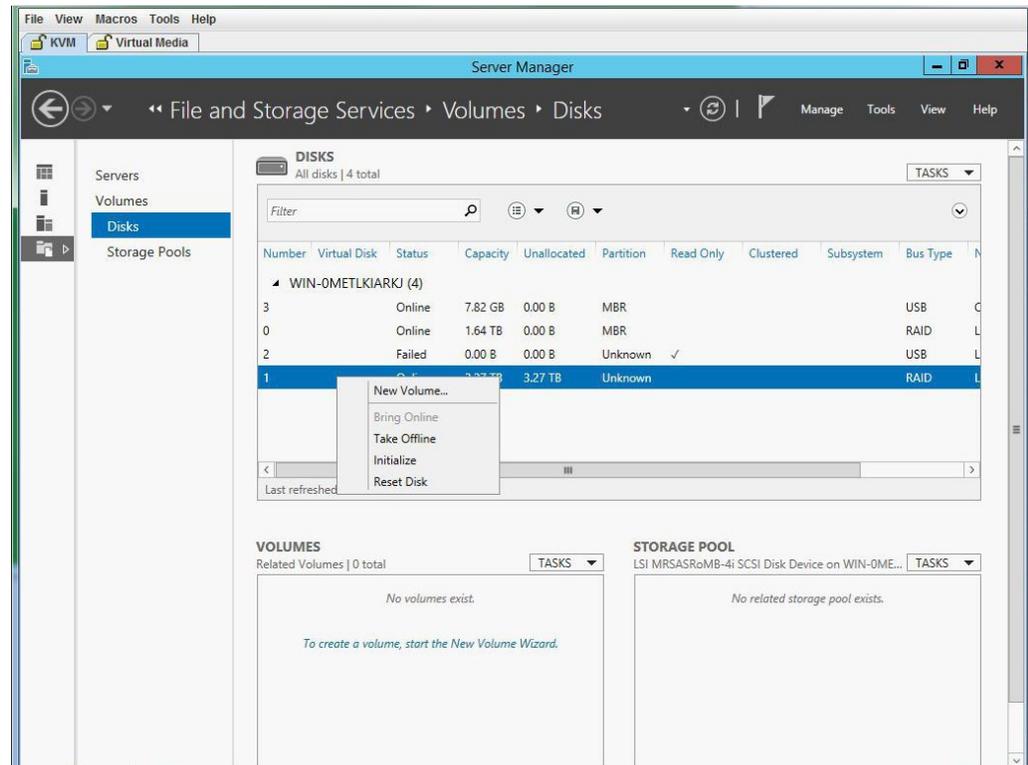
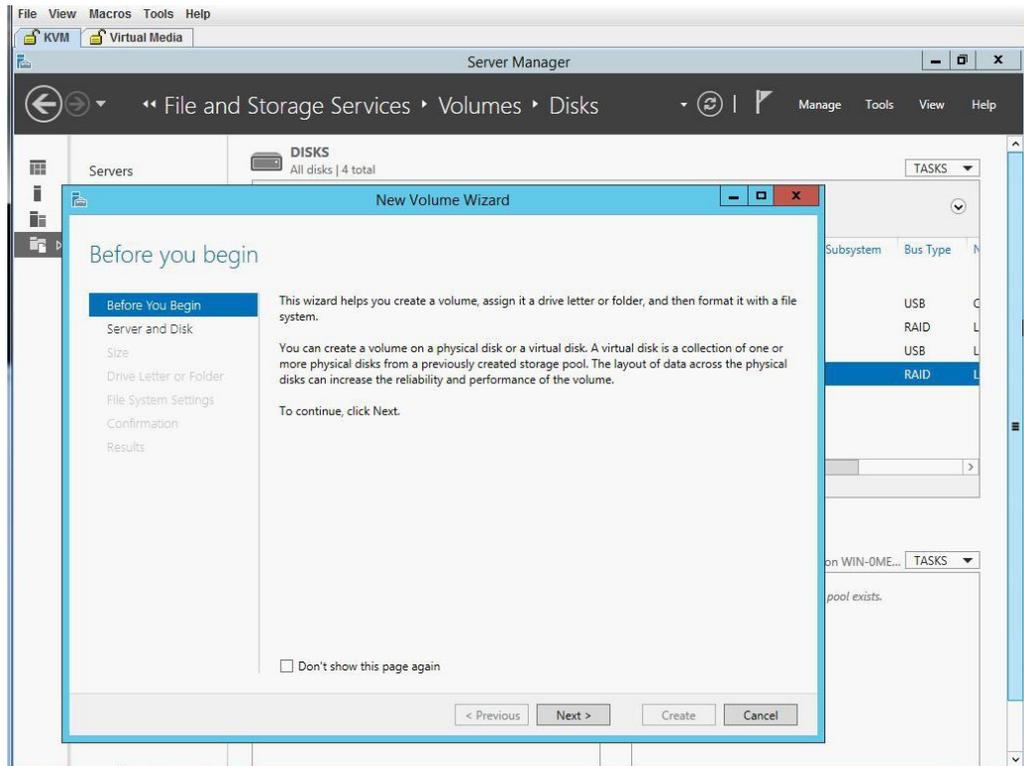
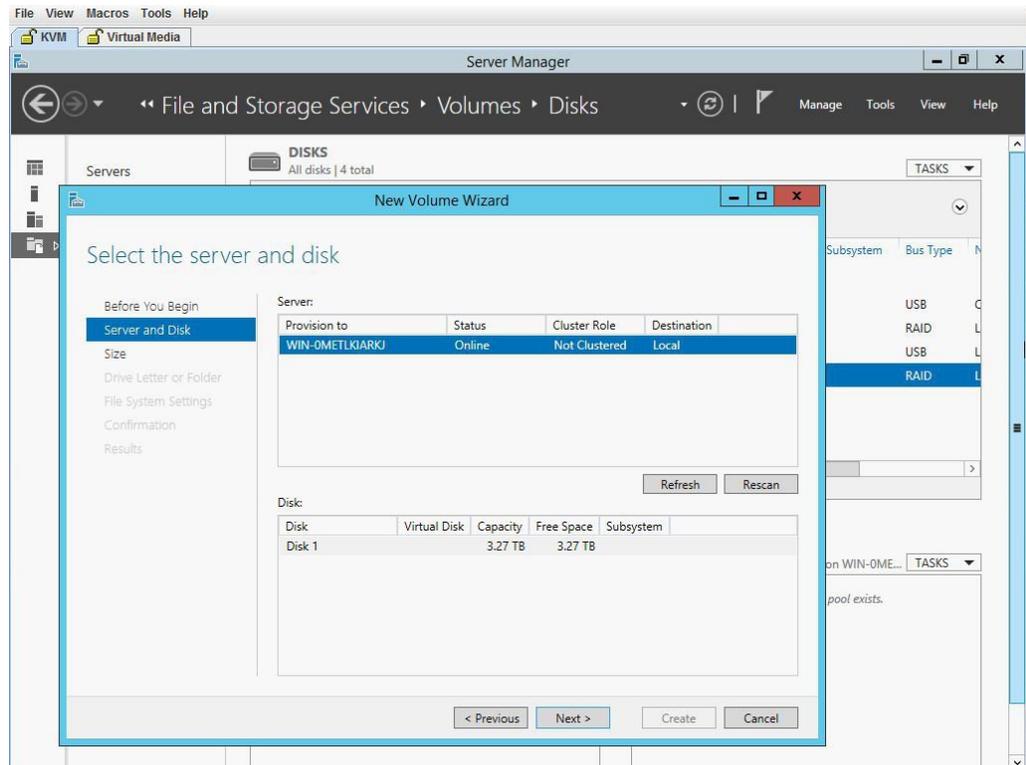


図 20 : [New Volume] ウィザード



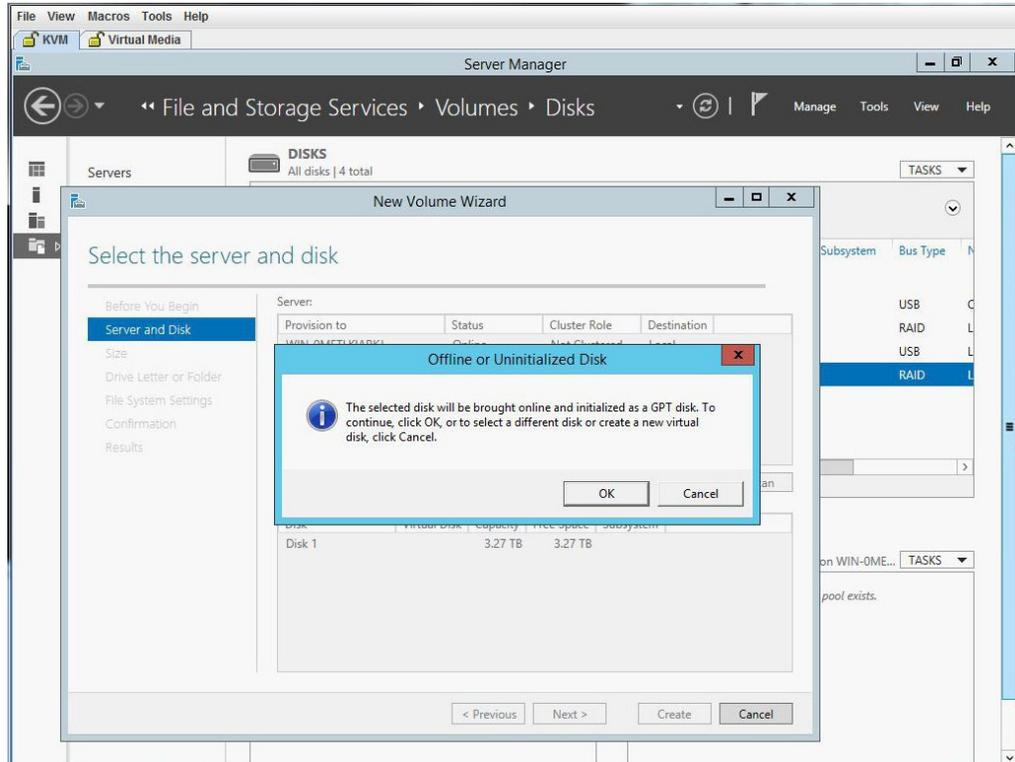
ステップ 13 サーバとディスクを選択し、[Next] をクリックします。確認のダイアログボックスが表示されま

図 21 : サーバとディスク



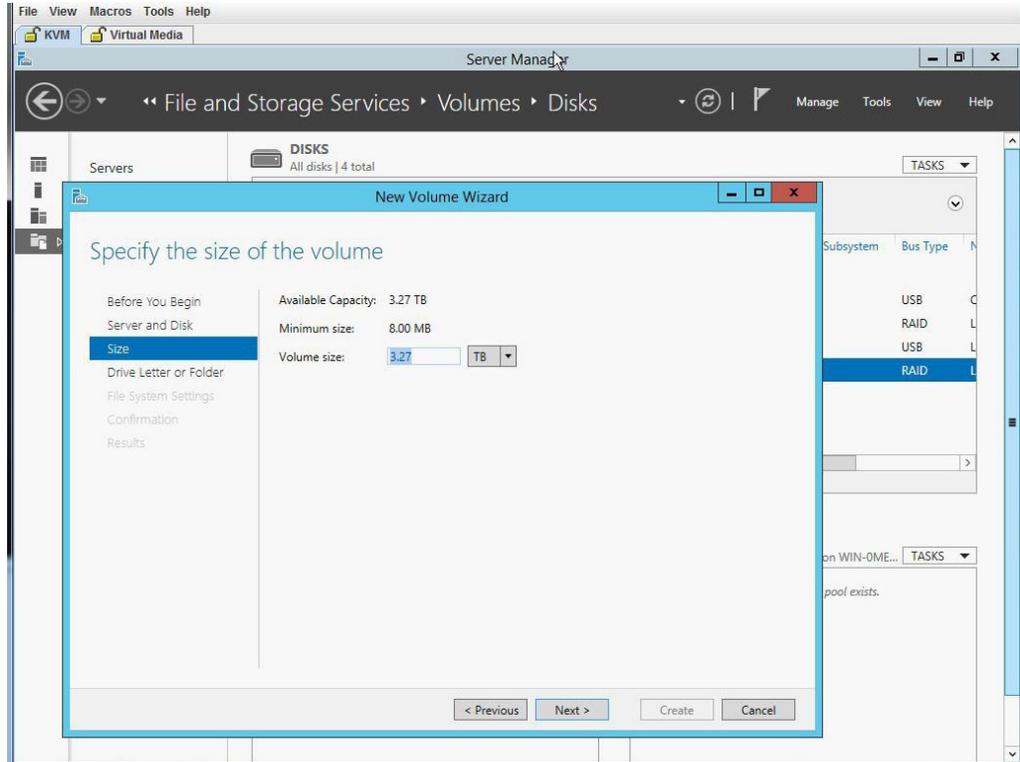
ステップ 14 [OK] をクリックします。

図 22: サーバとディスク



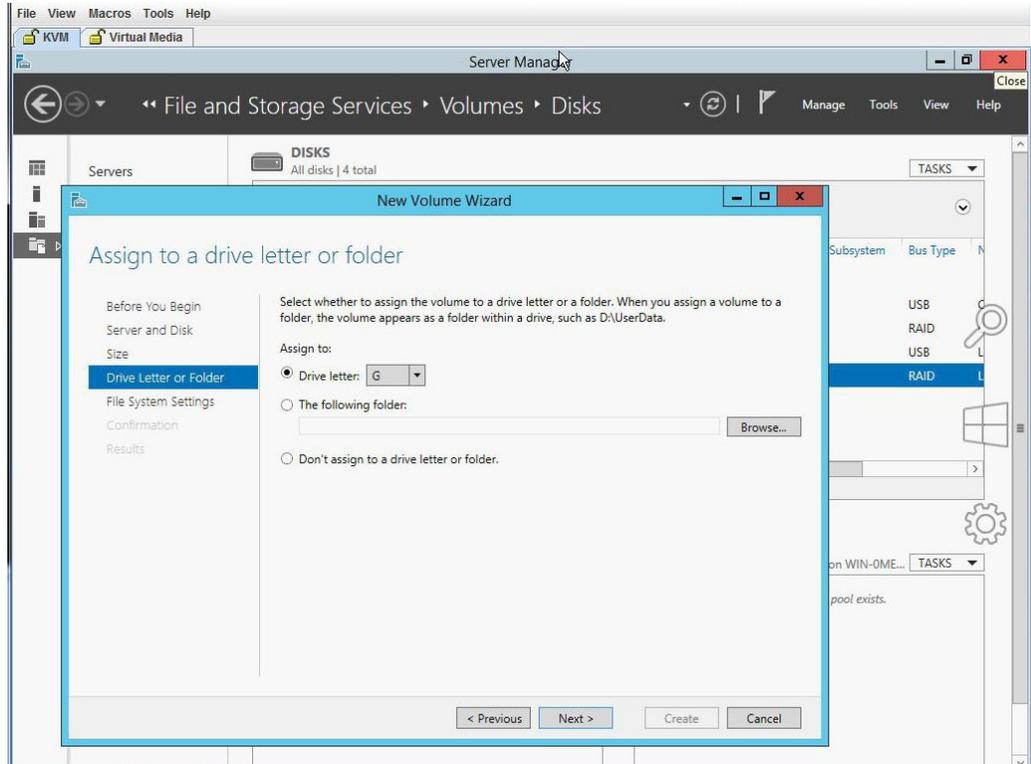
ステップ 15 ディスク ボリュームのサイズを指定します。

図 23: ディスク ボリュームのサイズ



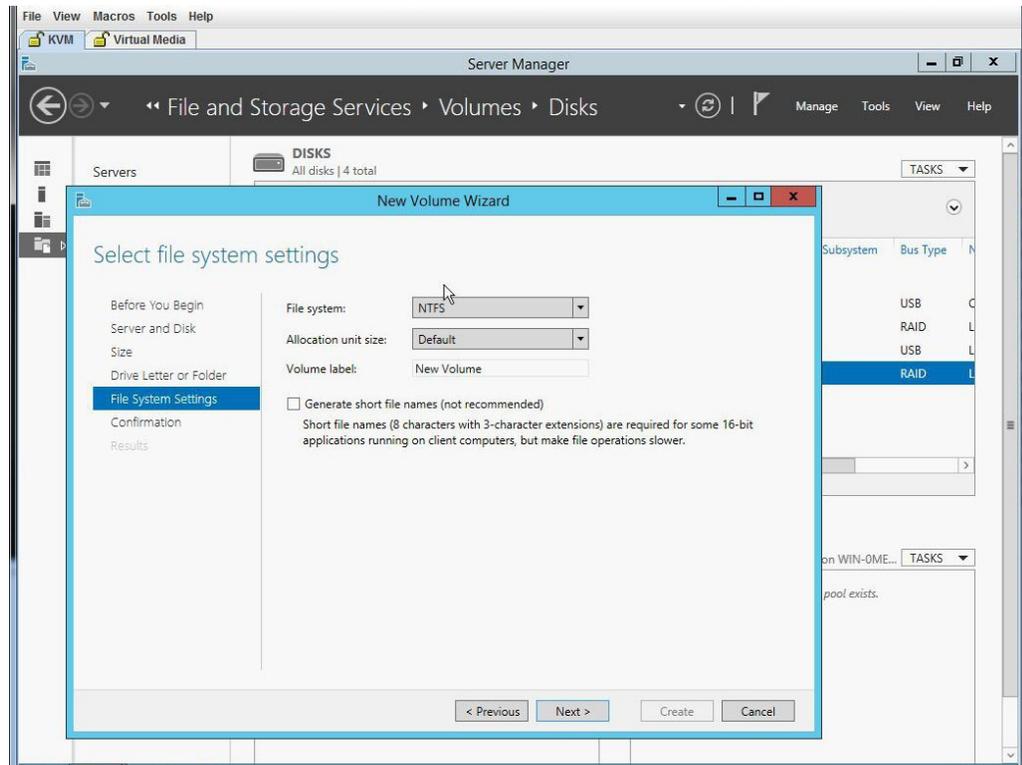
ステップ 16 ボリュームにドライブ文字を割り当てます。

図 24: ドライブ文字またはフォルダ



ステップ 17 ファイルシステムの設定を選択します。

図 25: ファイルシステムの設定



ステップ 18 選択内容を確認して、[Create] をクリックします。完了メッセージが表示されます。[Close] をクリックします。

図 26 : 選択内容の確認

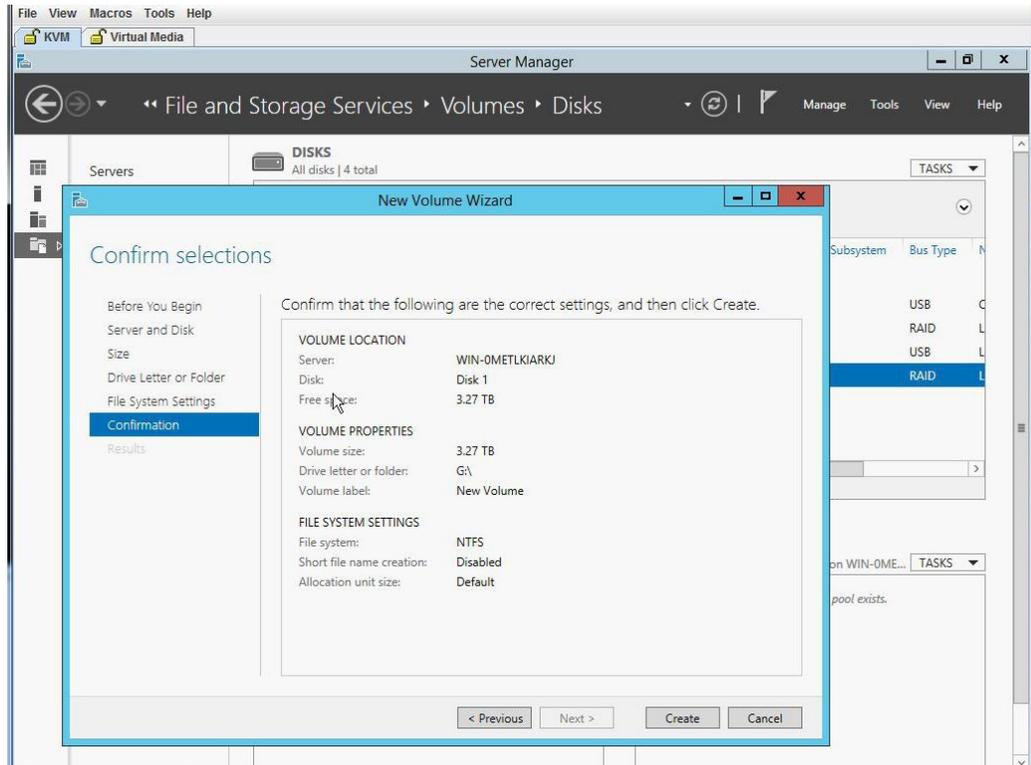
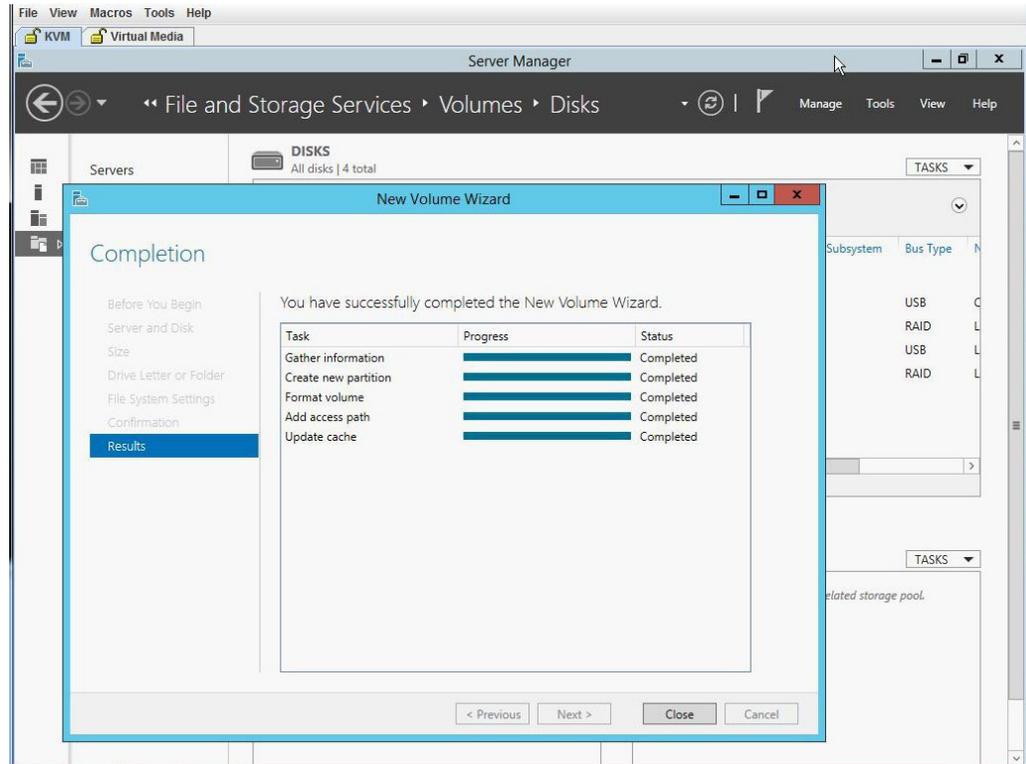
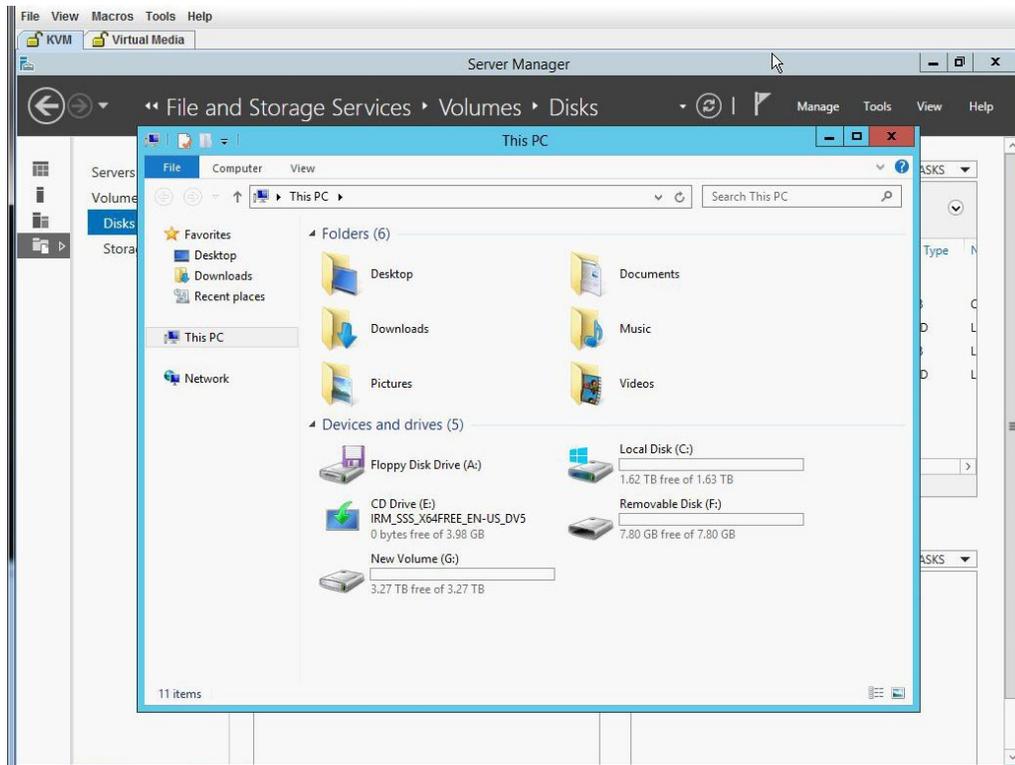


図 27 : Completion



ステップ 19 新しいボリュームが作成され、W2K12 が残りのストレージを認識していることを確認します。

図 28: 新しいボリュームの確認



2 TB を超える RAID ボリュームをサポートするための、UEFI を使用した W2K12 のインストール

この回避策では、2TB を超える RAID ボリュームをサポートするための、UEFI を使用した W2K12 のインストール方法を示します。この回避策には、次の主要なタスクが含まれます。

- 1 すべてのドライブを「Unconfigured Good」状態に設定します。
- 2 すべてのハードディスクを使用して仮想ドライブ 0 (VD0) を設定し、RAID0 に配置します。W2K12 が VD0 にインストールされ、OS がストレージ全体の容量を認識します。
- 3 BIOS セットアップを開始し、UEFI を使用して起動するように設定します。
- 4 ホストイメージマッピングを使用して W2K12 ISO をマッピングするか、vKVM を使用して仮想メディアをマッピングします。
- 5 EFI シェルに UCS E モジュールをブートします。

- 6 EFI シェルから、ISO およびブート BOOTX64.EFI に移動します。
- 7 W2K12 をインストールします。W2K12 のインストール中に、サーバが再起動します。
- 8 BIOS セットアップを開始し、[UCSM boot order rules] を [Strict] から [Loose] に変更します。この変更により、CIMC による BIOS のブート順序のオーバーライドが無効になり、BIOS のブート順序が、CIMC のブート順序の代わりに使用されます。
- 9 「Windows Boot Manager」をブート順序の一番上に移動します。これで、W2K12 は自動的に起動して、ストレージ全体を認識するようになります。

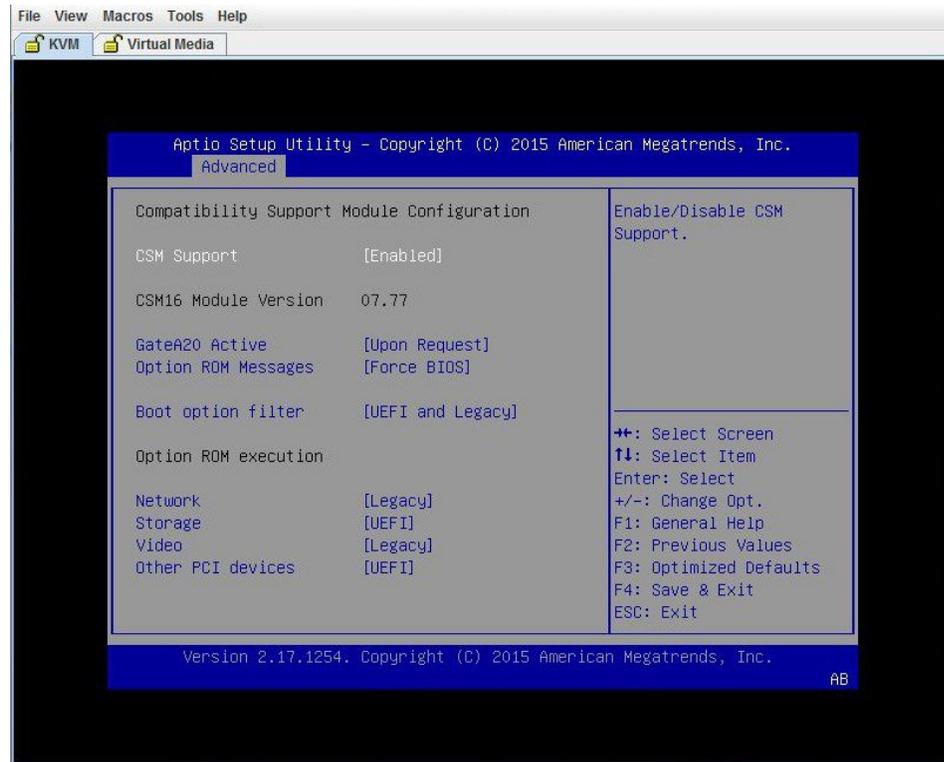
詳細な手順は次のとおりです。

手順

-
- ステップ 1 すべてのドライブを「Unconfigured Good」状態に設定します。参照 [物理ドライブの状態の変更](#), (60 ページ)
 - ステップ 2 すべてのハードディスクを使用して仮想ドライブ 0 (VD0) を設定し、RAID 0 に配置します。W2K12 が VD0 にインストールされ、OS がストレージ全体の容量を認識します。手順については次を参照してください。 [2 TB を超える RAID ボリュームをサポートするための、レガシー BIOS を使用した W2K12 のインストール](#), (71 ページ)
 - ステップ 3 BIOS セットアップを開始し、ストレージを [UEFI only] に変更します。

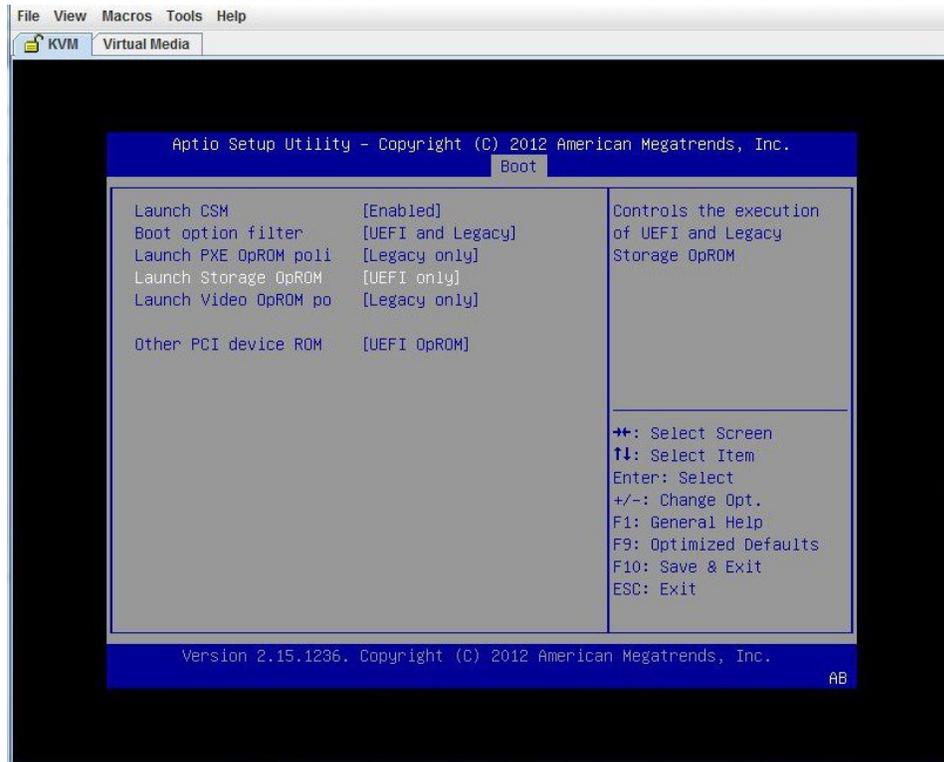
- a) Cisco UCS M3 サーバで、[Advanced] > [CSM] > [Option ROM execution] > [Storage] に移動し、[UEFI] を選択します。

図 29: BIOS セットアップの設定



- b) Cisco UCS M2 サーバで、[Boot] > [Launch Storage] > [OpROM] に移動し、[UEFI only] を選択します。

図 30: BIOS セットアップの設定



- ステップ 4** 仮想メディアを使用して ISO をマッピングするか、またはホストイメージマッピングを使用します。CIMC GUI を使用して、最初のブート可能デバイスとして「CD/DVD」を設定します。
- ステップ 5** サーバの電源を再投入します。起動時に F2 を押します。BIOS セットアップを開始し、EFI シェルに対するワнтаイム ブートを選択します。
- ステップ 6** EFI シェルから起動します。「Removable CDRom」を含んでいるファイルシステム番号 (fs#) を見つけます。

図 31 : EFI シェルからの起動

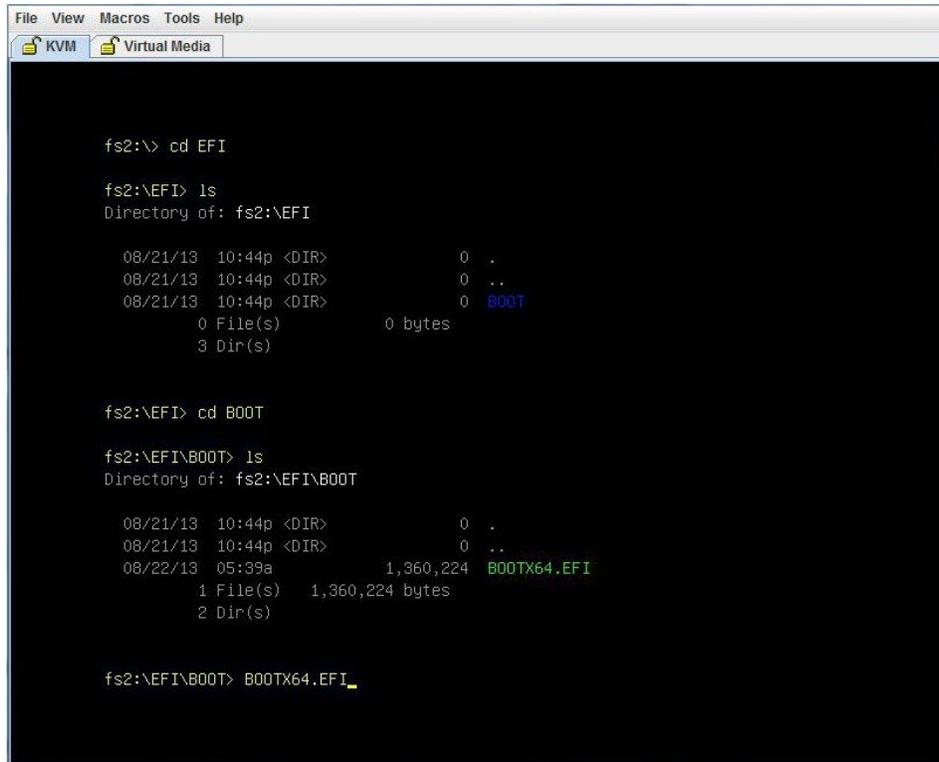
```

File View Macros Tools Help
KVM Virtual Media

fs2      :Removable CDRom - Alias cd26b0c0b blk2
         PciRoot(0x0)/Pci(0x1a,0x0)/USB(0x1,0x0)/USB(0x2,0x0)/CDROM(0x1,0x878,
0x1fe25e)
blk0     :Removable HardDisk - Alias hd16a0c fs0
         PciRoot(0x0)/Pci(0x3,0x2)/Pci(0x0,0x0)/Ctrl(0x0)/Scsi(0x0,0x0)/HD(2,G
PT,16ee7b95-7015-4f95-be91-422add7b736b,0x96800,0x32000)
blk1     :Removable HardDisk - Alias hd91b0f0b fs1
         PciRoot(0x0)/Pci(0x1d,0x0)/USB(0x1,0x0)/USB(0x5,0x0)/HD(1,MBR,0x00000
000,0x2000,0xf9f800)
blk2     :Removable CDRom - Alias cd26b0c0b fs2
         PciRoot(0x0)/Pci(0x1a,0x0)/USB(0x1,0x0)/USB(0x2,0x0)/CDROM(0x1,0x878,
0x1fe25e)
blk3     :Removable HardDisk - Alias (null)
         PciRoot(0x0)/Pci(0x3,0x2)/Pci(0x0,0x0)/Ctrl(0x0)/Scsi(0x0,0x0)/HD(1,G
PT,8a096920-a527-4cb9-bedb-53da6813a065,0x800,0x96000)
blk4     :Removable HardDisk - Alias (null)
         PciRoot(0x0)/Pci(0x3,0x2)/Pci(0x0,0x0)/Ctrl(0x0)/Scsi(0x0,0x0)/HD(3,G
PT,3a21c3c6-98ab-4d87-98ce-e2b6e0649c3e,0xc8800,0x40000)
blk5     :Removable HardDisk - Alias (null)
         PciRoot(0x0)/Pci(0x3,0x2)/Pci(0x0,0x0)/Ctrl(0x0)/Scsi(0x0,0x0)/HD(4,G
PT,e4d4f652-9e2d-46d7-856d-1c83aec28ed9,0x108800,0x2747b7000)
blk6     :Removable CDRom - Alias (null)
         PciRoot(0x0)/Pci(0x1a,0x0)/USB(0x1,0x0)/USB(0x2,0x0)/CDROM(0x0,0x876,
0x8)
blk7     :Removable BlockDevice - Alias (null)

```

図 32 : EFI シェルからの起動



```
File View Macros Tools Help
KVM Virtual Media

fs2:\> cd EFI

fs2:\EFI> ls
Directory of: fs2:\EFI

08/21/13 10:44p <DIR>          0 .
08/21/13 10:44p <DIR>          0 ..
08/21/13 10:44p <DIR>          0 B00T
0 File(s) 0 bytes
3 Dir(s)

fs2:\EFI> cd B00T

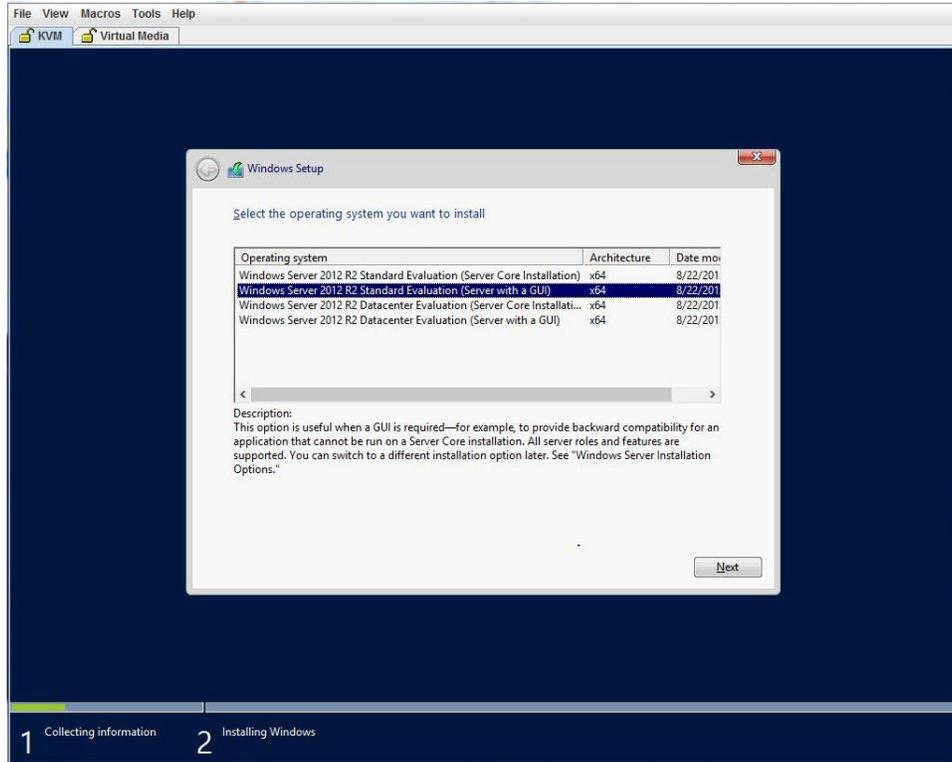
fs2:\EFI\B00T> ls
Directory of: fs2:\EFI\B00T

08/21/13 10:44p <DIR>          0 .
08/21/13 10:44p <DIR>          0 ..
08/22/13 05:39a              1,360,224 B00TX64.EFI
1 File(s) 1,360,224 bytes
2 Dir(s)

fs2:\EFI\B00T> B00TX64.EFI_
```

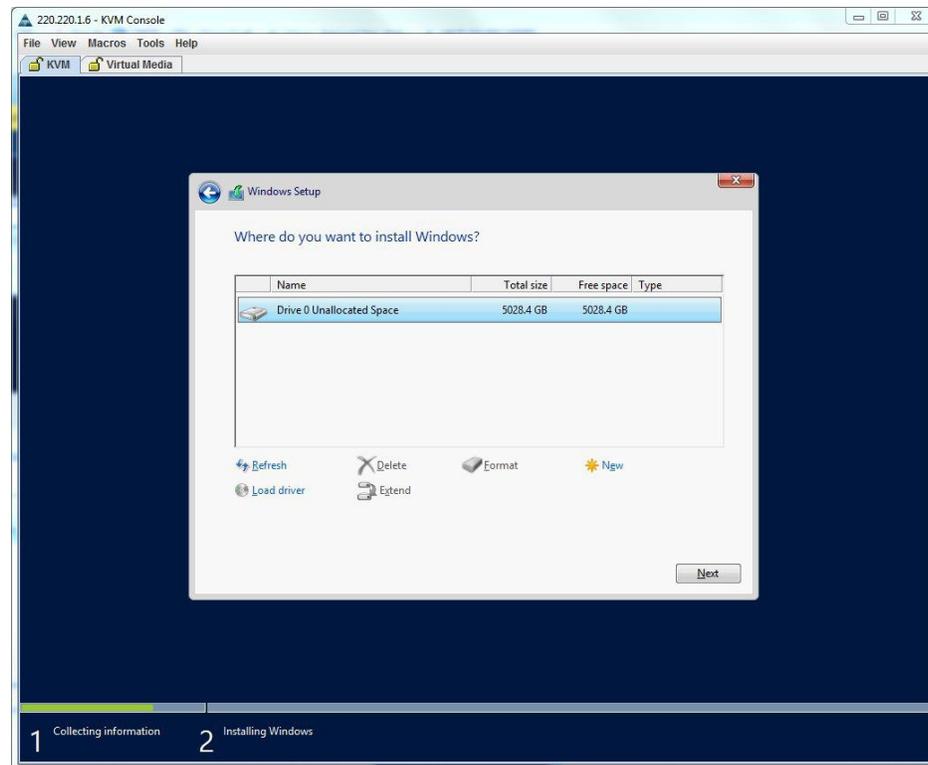
ステップ 7 GUI を使用して [W2K12 Standard Evaluation Server] を選択します。[Next] をクリックします。

図 33: Windows サーバのインストール



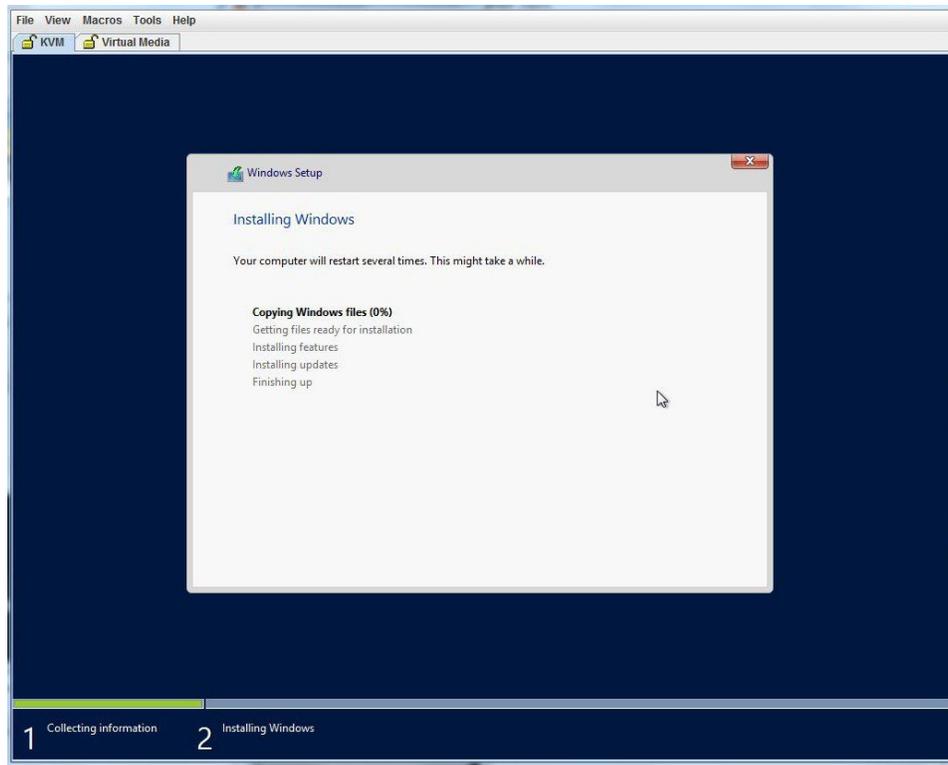
ステップ 8 Windows をインストールするドライブを選択します。[Next] をクリックします。

図 34 : Windows サーバのインストール



ステップ 9 インストールが完了するまで待機します。

図 35: **Windows** サーバのインストール



- ステップ 10** インストール後、(F2 を押して) BIOS セットアップを開始するか、(F6 を押して) [BIOS Boot] メニューを開き、Windows Boot Manager を使用して起動します。複数の Windows Boot Manager が表示される場合は、機能するものを選択します。

図 36: *Windows Boot Manager* を使用した *F2 BIOS* セットアップからの起動

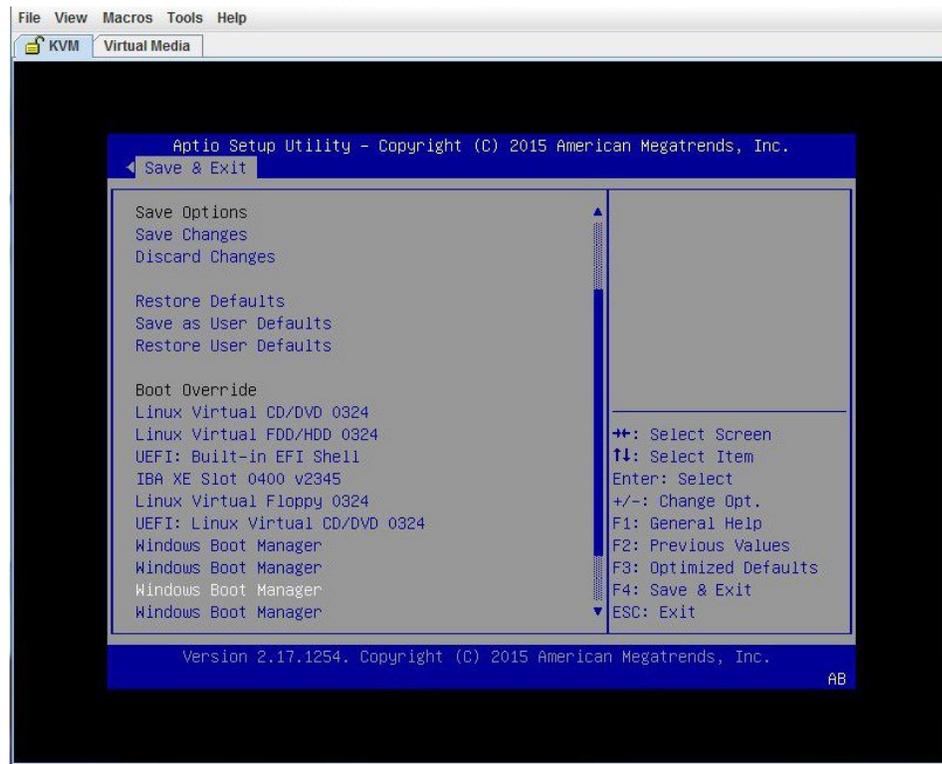
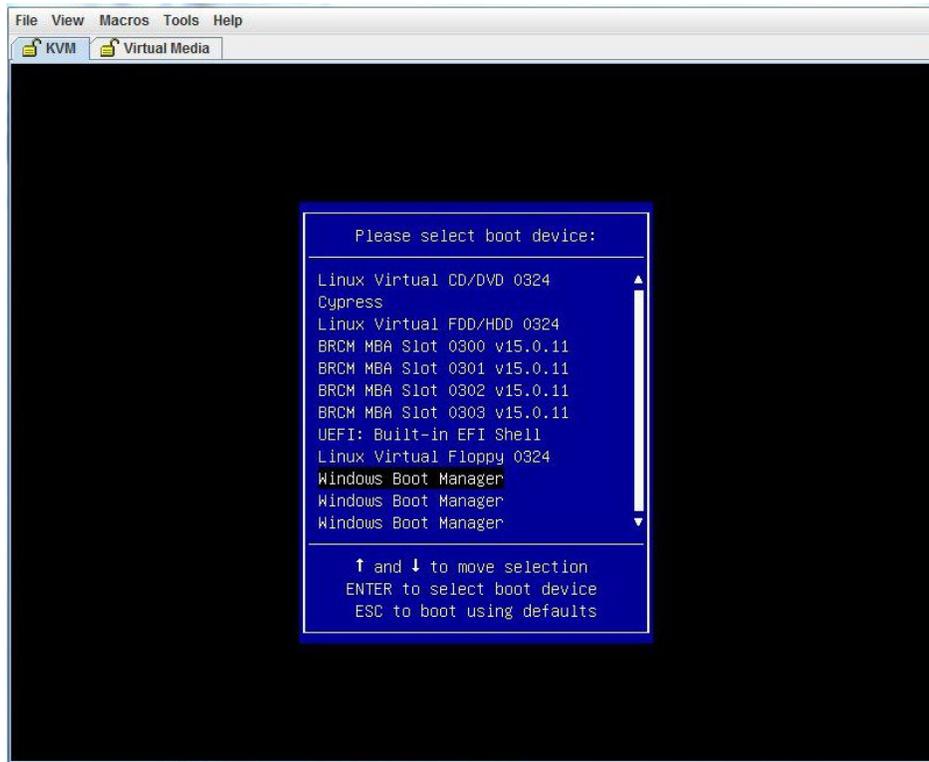
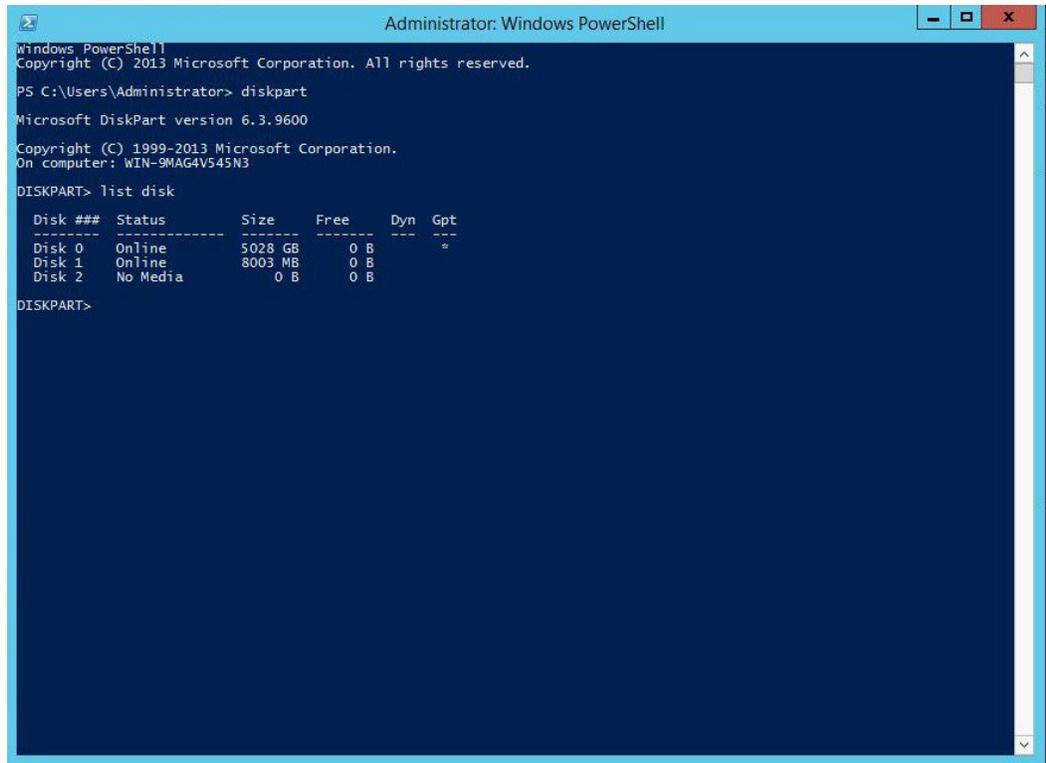


図 37: *Windows Boot Manager* を使用した *F6 [BIOS Boot]* メニューからの起動

ステップ 11 W2K12 が起動したら、**diskpart** コマンドを使用して GPT ボリュームを確認します。

図 38: GPT ボリュームの確認



```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> diskpart

Microsoft DiskPart version 6.3.9600

Copyright (C) 1999-2013 Microsoft Corporation.
On computer: WIN-9MAG4V543N3

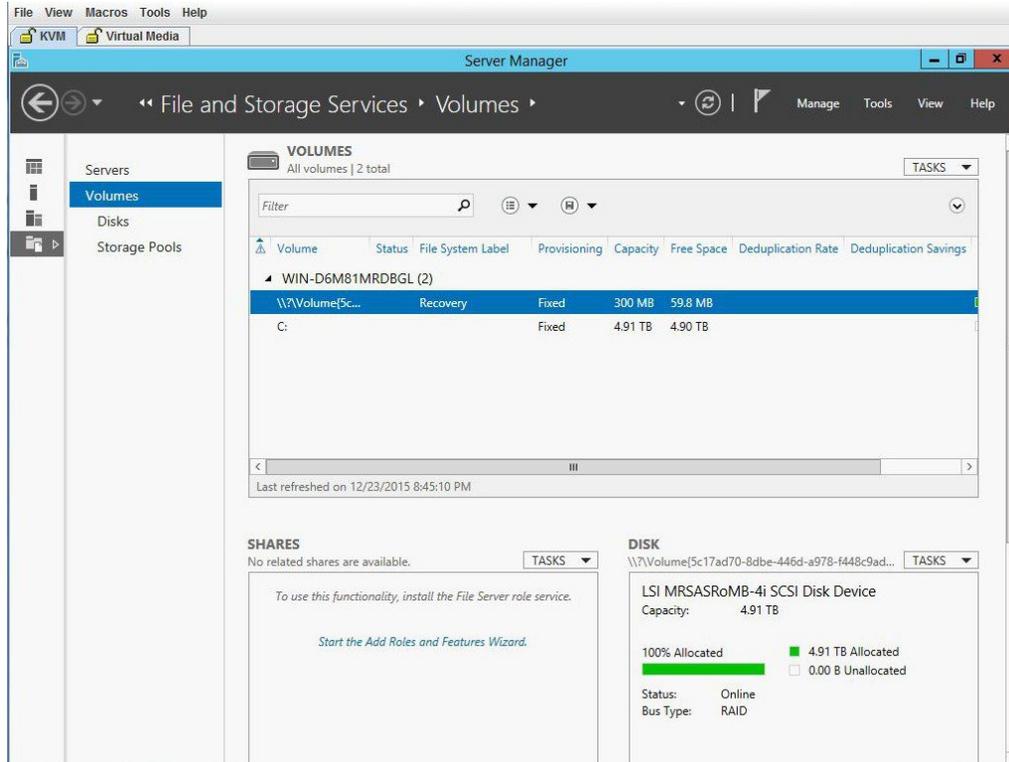
DISKPART> list disk

Disk ###  Status             Size             Free             Dyn             Gpt
-----  -
Disk 0    Online             5028 GB          0 B              *              *
Disk 1    Online             8003 MB          0 B              *              *
Disk 2    No Media           0 B              0 B              *              *

DISKPART>
```

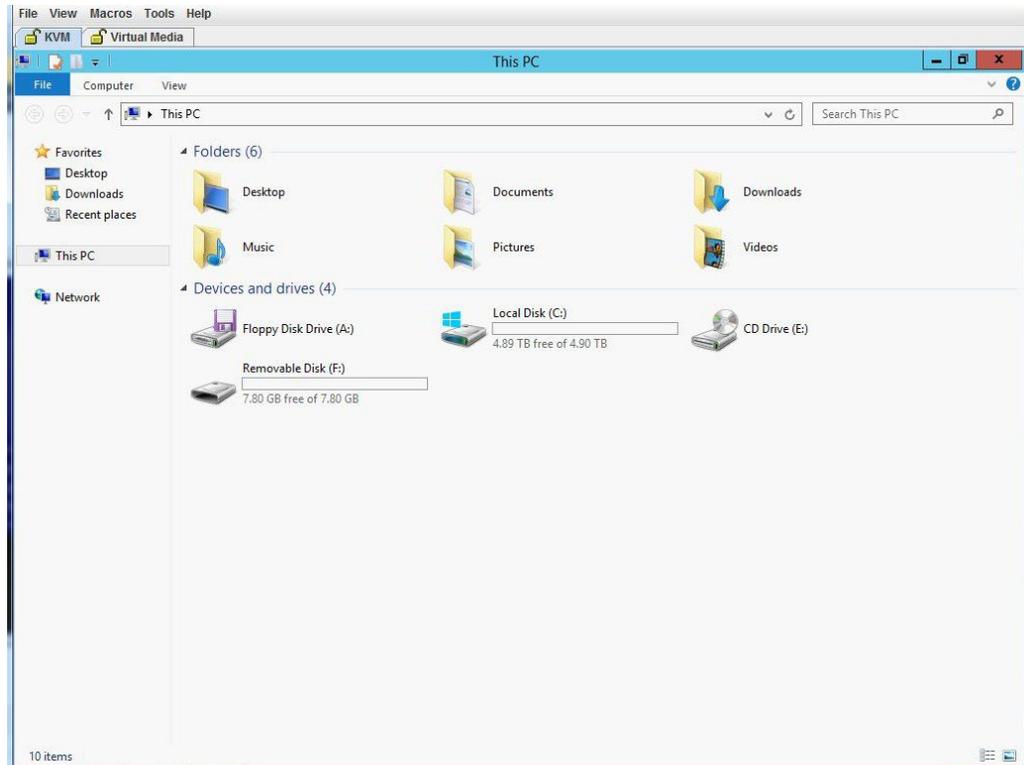
ステップ 12 W2K12 がボリューム全体を認識していることを確認します。

図 39: ボリュームの確認



ステップ 13 W2K12 が C ドライブの全ストレージを認識していることを確認します。

図 40 : ストレージ容量の確認

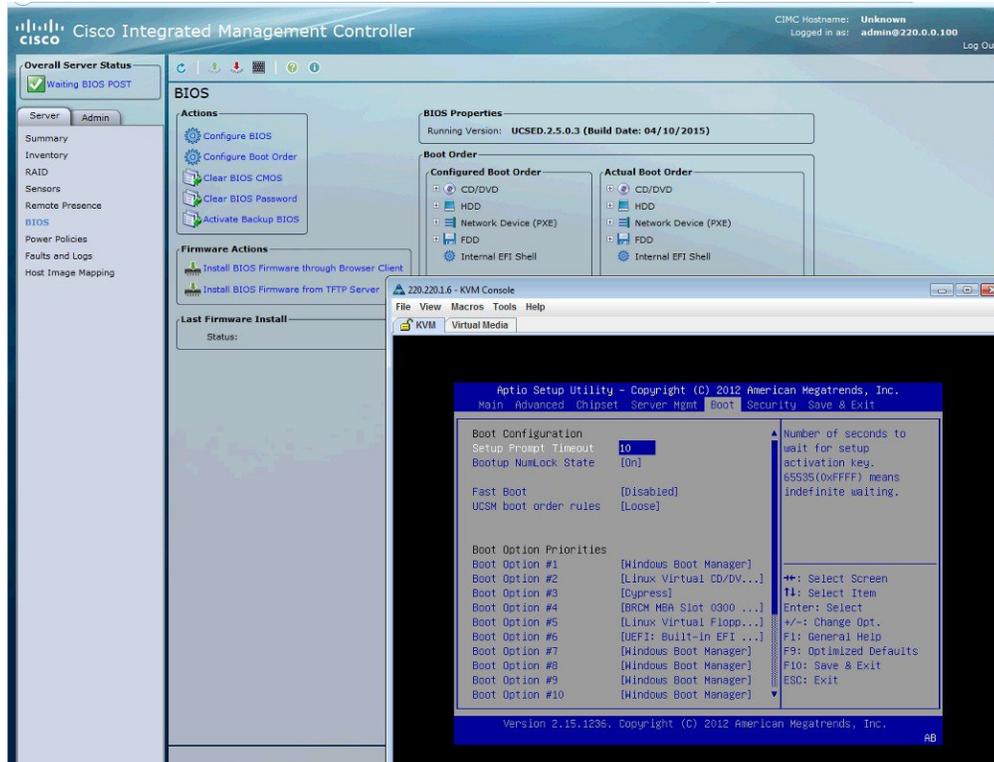


ステップ 14 W2K12 を自動的に起動するには、BIOS セットアップを開始して、次の変更を加えます。

- a) [UCSM boot order rules] を [Strict] から [Loose] に変更します。この変更により、CIMC による BIOS のブート順序のオーバーライドが無効になり、BIOS のブート順序が、CIMC のブート順序の代わりに使用されます。

- b) 「Windows Boot Manager」をブート順序の一番上に移動します。

図 41 : BIOS 設定



ステップ 15 最後に、変更内容を保存して BIOS セットアップを終了します。



第 5 章

サーバのプロパティの表示

この章は、次の項で構成されています。

- [サーバのプロパティの表示, 103 ページ](#)
- [CIMC 情報の表示, 104 ページ](#)
- [ルータ情報の表示, 105 ページ](#)
- [CPU のプロパティの表示, 105 ページ](#)
- [メモリのプロパティの表示, 106 ページ](#)
- [電源のプロパティの表示, 109 ページ](#)
- [ストレージのプロパティの表示, 109 ページ](#)
- [PCI アダプタのプロパティの表示, 111 ページ](#)
- [電力統計情報の表示, 112 ページ](#)
- [インターフェイスの MAC アドレスの表示, 112 ページ](#)
- [CIMC ネットワーク接続の状態の表示, 113 ページ](#)

サーバのプロパティの表示

手順

- ステップ 1** [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2** 作業ウィンドウの [Host Image Mapping] タブをクリックします。
- ステップ 3** [Server Summary] ペインの [Server Properties] 領域で、次の情報を確認します。

名前	説明
[Product Name] フィールド	サーバのモデル名。

名前	説明
[Serial Number] フィールド	サーバのシリアル番号。
[PID] フィールド	製品 ID。
[UUID] フィールド	サーバに割り当てられている UUID。
[BIOS Version] フィールド	サーバで実行されている BIOS のバージョン。
[Description] フィールド	サーバのユーザ定義の説明。

CIMC 情報の表示

手順

- ステップ 1** [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2** 作業ウィンドウの [Host Image Mapping] タブをクリックします。
- ステップ 3** [Server Summary] ペインの [Cisco Integrated Management Controller (CIMC) Information] 領域で、次の情報を確認します。

名前	説明
[Hostname] フィールド	CIMC のユーザ定義のホスト名。
[IP Address] フィールド	CIMC の IP アドレス。
[MAC Address] フィールド	CIMC に対するアクティブなネットワーク インターフェイスに割り当てられている MAC アドレス。
[Firmware Version] フィールド	現在の CIMC ファームウェアのバージョン。
[CPLD Version] フィールド	プログラマブルハードウェア論理バージョン。
[Hardware Version] フィールド	プリント基板バージョン。
[Current Time] フィールド	CIMC クロックが示している現在の日時。

ルータ情報の表示

手順

- ステップ 1** [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2** 作業ウィンドウの [Host Image Mapping] タブをクリックします。
- ステップ 3** [Server Summary] ペインの [Router Information] 領域で、次の情報を確認します。

名前	説明
[Router Model] フィールド	ルータのモデル番号。
[Serial Number] フィールド	ルータのシリアル番号
[Slot Number] フィールド	サーバがインストールされたルータのスロット番号。

CPU のプロパティの表示

手順

- ステップ 1** [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2** [Server] タブの [Inventory] をクリックします。
- ステップ 3** [Inventory] ペインの [CPUs] タブをクリックします。
- ステップ 4** 各 CPU で次の情報を確認します。

名前	説明
[Socket Name] フィールド	CPU が装着されているソケット
[Vendor] フィールド	CPU のベンダー
[Status] フィールド	CPU のステータス。
[Family] フィールド	この CPU が属するファミリー。
[Speed] フィールド	CPU の速度（メガヘルツ単位）。

名前	説明
[Version] フィールド	CPU のバージョン
[Number of Cores] フィールド	CPU のコアの数
[Signature] フィールド	CPU の署名情報。
[Number of Threads] フィールド	CPU が同時に処理できる最大スレッド数

メモリのプロパティの表示

手順

- ステップ 1** [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2** [Server] タブの [Inventory] をクリックします。
- ステップ 3** [Inventory] ペインの [Memory] タブをクリックします。
- ステップ 4** [Memory Summary] 領域で、メモリに関する次のサマリー情報を確認します。
E シリーズ サーバおよび SM E シリーズ NCE に表示されます。EHWIC E シリーズ NCE および NIM E シリーズ NCE には表示されません。

名前	説明
[Memory Speed] フィールド	メモリ速度 (メガヘルツ単位)。
[Failed Memory] フィールド	現在障害が発生しているメモリの量 (メガバイト単位)。
[Total Memory] フィールド	すべての DIMM が完全に機能している場合に、サーバで使用できるメモリの合計量。
[Ignored Memory] フィールド	現在使用できないメモリの量 (メガバイト単位)。
[Effective Memory] フィールド	現在サーバが使用できる実際のメモリの量。
[Number of Ignored DIMMs] フィールド	サーバがアクセスできない DIMM の数。
[Redundant Memory] フィールド	冗長ストレージに使用されるメモリの量。

名前	説明
[Number of Failed DIMMs] フィールド	障害が発生し、使用できない DIMM の数。
[Memory RAS Possible] フィールド	サーバがサポートするメモリ設定の詳細。次のいずれかになります。 <ul style="list-style-type: none"> • Memory configuration can support mirroring • Memory configuration can support sparing • Memory configuration can support either mirroring or sparing • Memory configuration can support lockstep • Memory configuration cannot support RAS
[Memory Configuration] フィールド	現在のメモリ設定。次のいずれかになります。 <ul style="list-style-type: none"> • [Maximum Performance] : システムは自動的にメモリのパフォーマンスを最適化します。 • [Mirroring] : サーバはメモリ内のデータのコピーを2つ保持します。このオプションによって、サーバ上の使用可能なメモリの半分がミラー化されたコピーに自動的に予約されるので、メモリを効果的に2等分できます。 • [Sparing] : システムは、DIMM に障害が発生した場合に使用するためのメモリを予約します。障害が発生した場合、サーバはDIMM をオフラインにして、予約済みのメモリと置き換えます。このオプションは、ミラーリングよりも冗長性が低くなりますが、サーバで実行するプログラムに使用できるメモリの量が多くなります。 • [Lockstep] : システムは、一度に2つのメモリチャネルを使用し、高いレベルの保護を提供します。このオプションは最も信頼性がありますが、合計メモリ容量が1/3減少します。
[DIMM Location Diagram]	物理サーバの DIMM の場所が表示されます。

ステップ 5

[Memory Details] テーブルで、各 DIMM に関する次の詳細情報を確認します。

ヒント カラムの見出しをクリックすると、そのカラムのエントリに従って表の行がソートされます。

名前	説明
[Name] カラム	メモリ モジュールが装着されている DIMM スロットの名前

名前	説明
[Capacity] カラム	DIMM のサイズ。
[Channel Speed] カラム	メモリ チャネルのクロック速度（メガヘルツ単位）。
[Channel Type] カラム	メモリ チャネルのタイプ。
[Memory Type Detail] カラム	デバイスで使用されるメモリのタイプ。
[Bank Locator] カラム	メモリ バンク内の DIMM の場所。
[Manufacturer] カラム	<p>製造業者のベンダー ID。次のいずれかになります。</p> <ul style="list-style-type: none"> • [0x2C00] : Micron Technology, Inc. • [0x5105] : Qimonda AG i. In. • [0x802C] : Micron Technology, Inc. • [0x80AD] : Hynix Semiconductor Inc. • [0x80CE] : Samsung Electronics, Inc. • [0x8551] : Qimonda AG i. In. • [0xAD00] : Hynix Semiconductor Inc. • [0xCE00] : Samsung Electronics, Inc.
[Serial Number] カラム	DIMM のシリアル番号。
[Part Number] カラム	ベンダーによって割り当てられた DIMM の部品番号。
[Visibility] カラム	DIMM がサーバに対して使用可能であるかどうか。
[Operability] カラム	DIMM が現在正常に動作しているかどうか。
[Data Width] カラム	DIMM がサポートするデータの量（ビット単位）。

電源のプロパティの表示

手順

- ステップ1 [Navigation] ペインの [Server] メニューをクリックします。
- ステップ2 [Server] タブの [Inventory] をクリックします。
- ステップ3 [Inventory] ペインの [Power Supplies] タブをクリックします。
- ステップ4 各電源で次の情報を確認します。
- ヒント カラムの見出しをクリックすると、そのカラムのエントリに従って表の行がソートされます。

名前	説明
[Device ID] カラム	電源装置ユニットの ID。
[Input] カラム	電源装置への入力 (ワット単位)。
[Max Output] カラム	電源装置からの最大出力 (ワット単位)。
[FW Version] カラム	電源装置のファームウェア バージョン。
[Product ID] カラム	ベンダーによって割り当てられた電源の製品識別子。

ストレージのプロパティの表示



- (注) この手順は E シリーズ サーバおよび S M E シリーズ NCE に適用されます。この手順は EHWIC E シリーズ NCE および NIM E シリーズ NCE には適用されません。

手順

- ステップ1 [Navigation] ペインの [Server] メニューをクリックします。
- ステップ2 [Server] タブの [RAID] をクリックします。
- ステップ3 [Storage Adapters] 領域で、使用可能なアダプタ カードに関する情報を確認します。

この領域には、CIMC を通じて管理できるサーバ上の RAID コントローラの一覧を示すテーブルが表示されます。特定のストレージデバイスの詳細を表示するには、テーブルからデバイスを選択し、下方のタブに情報を表示します。

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

ヒント カラムの見出しをクリックすると、そのカラムのエントリに従って表の行がソートされます。

ステップ 4 [Storage Adapters] 領域で、詳細なプロパティを表示するアダプタの行をクリックします。選択したストレージアダプタのプロパティが、[Storage Adapters] 領域の下のタブメニューに表示されます。

ステップ 5 [Controller Info] タブを選択し、情報を確認します。
[Storage Adapters] テーブルで RAID コントローラが選択されている場合、このタブに次の情報が表示されます。

- ファームウェアバージョン
- PCI 情報
- 実行中のファームウェア イメージ情報
- 仮想ドライブと物理ドライブの数
- 全般設定
- Capabilities
- ハードウェア構成
- エラー カウンタ

ステップ 6 [Physical Drive Info] タブを選択し、情報を確認します。
このタブには、[Storage Adapters] テーブルで選択したコントローラに関する次の情報が表示されます。

- 一般的なドライブ情報
- 識別情報
- ドライブ ステータス
- セキュリティ情報

ステップ 7 [Virtual Drive Info] タブを選択し、情報を確認します。
このタブには、[Storage Adapters] テーブルで選択したコントローラに関する次の情報が表示され、RAID 設定を作成、編集、またはクリアできます。

- 一般的なドライブ情報
- 物理ドライブ情報

PCI アダプタのプロパティの表示



(注) この手順はE シリーズ サーバおよび SME シリーズ NCE に適用されます。この手順は EHWIC E シリーズ NCE および NIM E シリーズ NCE には適用されません。

はじめる前に

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

手順

- ステップ 1 [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2 [Server] タブの [Inventory] をクリックします。
- ステップ 3 [Inventory] ペインの [PCI Adapters] タブをクリックします。
- ステップ 4 [PCI Adapters] 領域で、装着されている PCI アダプタの次の情報を確認します。

名前	説明
[Slot ID] カラム	アダプタが存在するスロット。
[Product Name] カラム	アダプタの名前。
[Firmware Version] カラム	現在の Cisco CIMC ファームウェアのバージョン。
[Vendor ID] カラム	ベンダーによって割り当てられたアダプタ ID。
[Sub Vendor ID] カラム	ベンダーによって割り当てられているセカンダリアダプタ ID。
[Device ID] カラム	ベンダーによって割り当てられたデバイス ID。
[Sub Device ID] カラム	ベンダーによって割り当てられているセカンダリデバイス ID。

電力統計情報の表示

手順

- ステップ 1 [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2 [Server] タブの [Power Policies] をクリックします。
- ステップ 3 [Power Statistics] 領域で、次のフィールドの情報を確認します。

名前	説明
[Current Consumption] フィールド	現在サーバによって使用されている電源（ワット単位）。
[Maximum Consumption] フィールド	最後にリポートされてからサーバが使用した最大ワット数。
[Minimum Consumption] フィールド	最後にリポートされてからサーバが使用した最小ワット数。

インターフェイスの MAC アドレスの表示

はじめる前に

システムで定義されたインターフェイスの名前、各インターフェイスに割り当てられた MAC アドレスを表示するには、管理者権限のあるユーザでログインする必要があります。

手順

- ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
- ステップ 2 [Admin] タブの [Network] をクリックします。
- ステップ 3 [Network] ペインの [Network Settings] タブをクリックします。
- ステップ 4 [LOMProperties] 領域で、システムで定義されたインターフェイスの名前、各インターフェイスに割り当てられた MAC アドレスを確認できます。

CIMC ネットワーク接続の状態の表示

はじめる前に

CIMC ネットワーク接続の状態を表示するには、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（リンクが検出されたかどうか、つまり物理ケーブルがネットワークインターフェイスに接続されているかどうか）。

手順

- ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
- ステップ 2 [Admin] タブの [Network] をクリックします。
- ステップ 3 [Network] ペインの [Network Settings] タブをクリックします。
- ステップ 4 [Link State] 領域で、次の情報を確認します。

名前	説明
[Interface] カラム	インターフェイスのシステム定義名。
[Link State] カラム	CIMC ネットワーク接続の状態。次のいずれかになります。 <ul style="list-style-type: none">• [Link Detected] : 物理ケーブルがネットワーク インターフェイスに接続されます。• [No Link Detected] : 物理ケーブルは、ネットワーク インターフェイスに接続されていません。



第 6 章

サーバのセンサーの表示

この章は、次の項で構成されています。

- [温度センサーの表示, 115 ページ](#)
- [電圧センサーの表示, 116 ページ](#)
- [LED センサーの表示, 117 ページ](#)
- [ストレージセンサーの表示, 118 ページ](#)

温度センサーの表示

手順

- ステップ 1** [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2** [Server] タブの [Sensors] をクリックします。
- ステップ 3** [Sensors] ペインの [Temperature] タブをクリックします。
- ステップ 4** サーバの温度に関する次の統計情報が表示されます。
- ヒント** カラムの見出しをクリックすると、そのカラムのエントリに従って表の行がソートされます。

名前	説明
[Sensor Name] カラム	センサーの名前。次のいずれかになります。 <ul style="list-style-type: none">• [TEMP_AMB_X] : モジュール内にあるセンサーから取得された周囲温度。• [P1_TEMP_SENS] : プロセッサ コア温度。• [DDR3_P1_X0_TMP] : メモリ モジュール温度。

名前	説明
[Status] カラム	センサーのステータス。次のいずれかになります。 <ul style="list-style-type: none"> • [Unknown] • [Informational] • [Normal] • [Warning] • [Critical] • [Non-Recoverable]
[Temperature] カラム	現在の温度（摂氏単位）。
[Warning Threshold Min] カラム	Warning の最小しきい値。
[Warning Threshold Max] カラム	Warning の最大しきい値。
[Critical Threshold Min] カラム	Critical の最小しきい値。
[Critical Threshold Max] カラム	Critical の最大しきい値。

電圧センサーの表示

手順

- ステップ 1 [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2 [Server] タブの [Sensors] をクリックします。
- ステップ 3 [Sensors] ペインの [Voltage] タブをクリックします。
- ステップ 4 サーバの電圧に関する次の統計情報が表示されます。
ヒント カラムの見出しをクリックすると、そのカラムのエントリに従って表の行がソートされます。

名前	説明
[Sensor Name] カラム	センサーの名前。

名前	説明
[Status] カラム	センサーのステータス。次のいずれかになります。 <ul style="list-style-type: none"> • [Unknown] • [Informational] • [Normal] • [Warning] • [Critical] • [Non-Recoverable]
[Voltage] カラム	現在の電圧（ボルト単位）。
[Warning Threshold Min] カラム	Warning の最小しきい値。
[Warning Threshold Max] カラム	Warning の最大しきい値。
[Critical Threshold Min] カラム	Critical の最小しきい値。
[Critical Threshold Max] カラム	Critical の最大しきい値。

LED センサーの表示

手順

- ステップ 1 [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2 [Server] タブの [Sensors] をクリックします。
- ステップ 3 [Sensors] ペインの [LEDs] タブをクリックします。
- ステップ 4 サーバの LED に関する次の統計情報が表示されます。

名前	説明
[Sensor Name] カラム	<p>センサーの名前。次のいずれかになります。</p> <ul style="list-style-type: none"> • [LED_HLTH_STATUS] : システム全体の状態を示すステータスセンサー（物理 LED ではない）。 • [LED_DIMM_STATUS] : DIMM の状態を示すステータスセンサー（物理 LED ではない）。 • [LED_CPU_STATUS] : CPU の状態を示すステータスセンサー（物理 LED ではない）。 • [LED_SYS_ACT] : システム アクティビティ。システムに電源が投入され、ブートが完了しているかどうかを示します。 （注） NIM E シリーズ NCE には表示されません。
[LED State] カラム	LED が点灯、点滅、または消灯しているかどうか。
[LED Color] カラム	<p>LED の現在のステータス。</p> <p>色の意味の詳細については、使用しているサーバタイプに対応するハードウェアインストールガイドを参照してください。</p>

ストレージセンサーの表示

手順

- ステップ 1 [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2 [Server] タブの [Sensors] をクリックします。
- ステップ 3 [Sensors] ペインの [Storage] タブをクリックします。
- ステップ 4 サーバのストレージに関する次の統計情報が表示されます。

名前	説明
[Name] カラム	<p>ストレージデバイスの名前。ここに表示される値は次のとおりです。</p> <p>[HDDX_PRS] : 各ハードドライブの有無を示します。</p>

名前	説明
[Status] カラム	ストレージデバイスのステータスの簡単な説明。
[LED Status] カラム	現在の LED の色（ある場合）。 ストレージデバイスの物理 LED を点滅させるには、ドロップダウンリストから [Turn On] を選択します。LED の点滅をストレージデバイスに制御させるには、[Turn Off] を選択します。



第 7 章

リモート プレゼンスの管理

この章は、次の項で構成されています。

- [仮想 KVM の管理, 121 ページ](#)
- [仮想メディアの設定, 124 ページ](#)
- [Serial over LAN の設定, 129 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、リモートの場合からサーバに接続できます。サーバに物理的に接続された CD/DVD ドライブまたはフロッピードライブを使用する代わりに、KVM コンソールは仮想メディアを使用します。これは、仮想 CD/DVD ドライブまたはフロッピードライブにマップされる実際のディスクドライブまたはディスクイメージファイルです。次のいずれでも仮想ドライブにマップできます。

- コンピュータ上の CD/DVD またはフロッピー ドライブ
- コンピュータ上のディスク イメージファイル (ISO または IMG ファイル)
- コンピュータ上の USB フラッシュ ドライブ

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

- ブートアップ中に F2 を押して、BIOS セットアップ メニューにアクセスします。
- ブートアップ中に F8 を押して、CIMC Configuration Utility にアクセスします。



(注) CIMC Configuration Utility は EHWIC E シリーズ NCE および NIM E シリーズ NCE には適用されません。

- Cisco UCS M1 および M2 サーバの場合は、ブートアップ中に Ctrl+H を押し、WebBIOS にアクセスして RAID を設定します。

Cisco UCS M3 サーバの場合は、ブートアップ中に Ctrl+R を押し、MegaRAID コントローラにアクセスして RAID を設定します。



(注) RAID は EHWIC E シリーズ NCE および NIM E シリーズ NCE ではサポートされていません。これらの SKU では、Ctrl+H および Ctrl+R は機能しません。

KVM コンソールを起動するための Java 要件

KVM コンソールを起動するためには、システムにリリース 1.6 以降の Java をインストールしておく必要があります。

証明書が Java で取り消されたために KVM コンソールが起動しない場合は、Java の設定を変更する必要があります。次の手順を実行します。

- 1 Java コントロールパネルにアクセスします。
- 2 [Advanced] タブをクリックします。
- 3 [Perform certificate revocation on] で、[Do not check (not recommended)] ラジオ ボタンを選択します。詳細については、http://www.java.com/en/download/help/revocation_options.xmlを参照してください。

仮想 KVM の設定

はじめる前に

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

手順

- ステップ 1 [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2 [Server] タブの [Remote Presence] をクリックします。
- ステップ 3 [Remote Presence] ペインの [Virtual KVM] タブをクリックします。
- ステップ 4 [vKVM Properties] 領域で、次のフィールドに値を入力します。

名前	説明
[Enabled] チェックボックス	オンにすると、仮想 KVM がイネーブルになります。 (注) 仮想メディアビューアには KVM を使用してアクセスします。KVM コンソールをディセーブルにすると、CIMC はホストに接続されているすべての仮想メディア デバイスへのアクセスもディセーブルにします。
[Max Sessions] ドロップダウン リスト	許可されている KVM の同時セッションの最大数。選択できる数値は 1 ~ 4 です。
[Active Sessions] フィールド	サーバで実行されている KVM セッションの数。
[Remote Port] フィールド	KVM 通信に使用するポート。
[Enable Video Encryption] チェックボックス	オンにすると、サーバは KVM で送信されるすべてのビデオ情報を暗号化します。
[Enable Local Server Video] チェックボックス (注) EHWIC E シリーズ NCE には表示されません。	オンにすると、KVM セッションはサーバに接続されているすべてのモニタにも表示されます。

ステップ 5 [Save Changes] をクリックします。

仮想 KVM のイネーブル化

はじめる前に

仮想 KVM をイネーブルにするには、admin 権限を持つユーザとしてログインする必要があります。

手順

- ステップ 1 [Navigation] ペインの [Server] メニューをクリックします。
 - ステップ 2 [Server] タブの [Remote Presence] をクリックします。
 - ステップ 3 [Remote Presence] ペインの [Virtual KVM] タブをクリックします。
 - ステップ 4 [vKVM Properties] 領域で、[Enabled] チェックボックスをオンにします。
 - ステップ 5 [Save Changes] をクリックします。
-

仮想 KVM のディセーブル化

はじめる前に

仮想 KVM をディセーブルにするには、admin 権限を持つユーザとしてログインする必要があります。

手順

- ステップ 1 [Navigation] ペインの [Server] メニューをクリックします。
 - ステップ 2 [Server] タブの [Remote Presence] をクリックします。
 - ステップ 3 [Remote Presence] ペインの [Virtual KVM] タブをクリックします。
 - ステップ 4 [vKVM Properties] 領域で、[Enabled] チェックボックスをオフにします。
 - ステップ 5 [Save Changes] をクリックします。
-

仮想メディアの設定

はじめる前に

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

手順

- ステップ 1 [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2 [Server] タブの [Remote Presence] をクリックします。
- ステップ 3 [Remote Presence] ペインの [Virtual Media] タブをクリックします。
- ステップ 4 [Virtual Media Properties] 領域で、次のプロパティを更新します。

名前	説明
[Enabled] チェックボックス	オンにすると、仮想メディアがイネーブルになります。 (注) このチェックボックスをオフにすると、すべての仮想メディア デバイスはホストから自動的に切断されます。
[Active Sessions] フィールド	現在実行されている仮想メディア セッションの数。
[Enable Virtual Media Encryption] チェックボックス	オンにすると、すべての仮想メディア通信は暗号化されます。
[Low Power USB enabled] チェックボックス	これを選択すると、低電力 USB が有効になります。 低電力 USB が有効化された場合、ISO をマッピングしてホストを再起動した後、ブート選択メニューに仮想ドライブが表示されます。ただし、UCS VIC P81E カードのあるサーバに ISO をマッピングするとき、NIC が Cisco Card モードである場合には、仮想ドライブがブート選択メニューに表示されるようにするには、このオプションを無効にする必要があります。

ステップ 5 [Save Changes] をクリックします。

CIMC マップされた vMedia ボリュームの作成

はじめる前に

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

手順

- ステップ 1 [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2 [Server] タブの [Remote Presence] をクリックします。
- ステップ 3 [Remote Presence] ペインの [Virtual Media] タブをクリックします。
- ステップ 4 [CIMC-Mapped vMedia] 領域で、[Add New Mapping] をクリックします。
- ステップ 5 [CIMC-Mapped vMedia] ダイアログボックスで、次のフィールドを更新します。

名前	説明
[Volume] フィールド	マッピング用にマウントされるイメージの ID。

名前	説明
[Mount Type] ドロップダウンリスト	マッピングのタイプ。次のいずれかになります。 <ul style="list-style-type: none">• [NFS] : ネットワーク ファイル システム。• [CIFS] : Common Internet File System。• [WWW(HTTP/HTTPS)] : HTTP ベースまたは HTTPS ベースのシステム。
[Remote Share] フィールド	マップするイメージの URL。形式は選択された [Mount Type] によって異なります。 <ul style="list-style-type: none">• [NFS] : serverip:/share を使用します。• [CIFS] : serverip://share を使用します。• [WWW(HTTP/HTTPS)] : http[s]://serverip/share を使用します。
[Remote File] フィールド	リモート共有の .iso または .img ファイルの名前と場所。

名前	説明
[Mount Options] フィールド	<p>カンマ区切りリストで入力される業界標準のマウントオプション。オプションは選択された [Mount Type] によって異なります。</p> <p>[NFS] を使用している場合は、このフィールドを空白のままにするか、次の中から 1 つ以上を入力します。</p> <ul style="list-style-type: none"> • ro • rw • nolock • noexec • soft • port=VALUE • timeo=VALUE • retry=VALUE <p>[CIFS] を使用している場合は、このフィールドを空白のままにするか、次の中から 1 つ以上を入力します。</p> <ul style="list-style-type: none"> • soft • nounix • noserverino • ゲスト • [username=VALUE] : guest が入力された場合は無視されます。 • [password=VALUE] : guest が入力された場合は無視されます。 <p>[WWW(HTTP/HTTPS)] を使用している場合は、このフィールドを空白のままにするか、次を入力します。</p> <ul style="list-style-type: none"> • noauto
[User Name] フィールド	選択された [Mount Type] のユーザ名 (必要な場合)。
[Password] フィールド	選択されたユーザ名のパスワード (必要な場合)。

ステップ 6 [Save (保存)] をクリックします。

CIMC マップされた vMedia ボリュームのプロパティの表示

はじめる前に

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

手順

- ステップ 1** [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2** [Server] タブの [Remote Presence] をクリックします。
- ステップ 3** [Remote Presence] ペインの [Virtual Media] タブをクリックします。
- ステップ 4** [CIMC-Mapped vMedia] 領域で、[Current Mappings] テーブルから行を選択します。
- ステップ 5** [Properties] をクリックし、次の情報を確認します。

名前	説明
[Volume] フィールド	マッピング用にマウントされるイメージの ID。
[Mount Type] ドロップダウンリスト	マッピングのタイプ。次のいずれかになります。 <ul style="list-style-type: none"> • [NFS] : ネットワーク ファイル システム。 • [CIFS] : Common Internet File System。 • [WWW(HTTP/HTTPS)] : HTTP ベースまたは HTTPS ベースのシステム。
[Remote Share] フィールド	マップするイメージの URL。
[Remote File] フィールド	リモート共有の .iso または .img ファイルの名前と場所。
[Mount Options] フィールド	選択されたマウント オプション。
[User Name] フィールド	ユーザ名 (ある場合)。
[Password] フィールド	選択されたユーザ名のパスワード (ある場合)。

CIMC マップされた vMedia ボリュームの削除

はじめる前に

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

手順

-
- ステップ 1 [Navigation] ペインの [Server] メニューをクリックします。
 - ステップ 2 [Server] タブの [Remote Presence] をクリックします。
 - ステップ 3 [Remote Presence] ペインの [Virtual Media] タブをクリックします。
 - ステップ 4 [CIMC-Mapped vMedia] 領域で、[Unmap] をクリックします。
-

Serial over LAN の設定

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



- (注) 一部のオペレーティング システム（Red Hat Enterprise Linux など）では、シリアル コンソールにリダイレクトするために追加の設定が必要です。

はじめる前に

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

手順

-
- ステップ 1 [Navigation] ペインの [Server] メニューをクリックします。
 - ステップ 2 [Server] タブの [Remote Presence] をクリックします。
 - ステップ 3 [Remote Presence] ペインの [Serial over LAN] タブをクリックします。
 - ステップ 4 [Serial over LAN Properties] 領域で、次のプロパティを更新します。

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

名前	説明
[Baud Rate] ドロップダウン リスト	システムが Serial over LAN 通信に使用するボー レート。次のいずれかを選択できます。 <ul style="list-style-type: none">• 9600 bps• 19.2 kbps• 38.4 kbps• 57.6 kbps• 115.2 kbps
[SSH Port] フィールド	セキュア シェル アクセスに使用するポート。デフォルトは 22 です。

ステップ 5 [Save Changes] をクリックします。



第 8 章

ユーザ アカウントの管理

この章は、次の項で構成されています。

- [ローカルユーザの設定, 131 ページ](#)
- [LDAP サーバ \(Active Directory\) , 132 ページ](#)
- [ユーザセッションの表示, 139 ページ](#)

ローカルユーザの設定

はじめる前に

ローカルユーザアカウントを設定または変更するには、**admin** 権限を持つユーザとしてログインする必要があります。

手順

- ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
- ステップ 2 [Admin] タブの [User Management] をクリックします。
- ステップ 3 [User Management] ペインの [Local User] タブをクリックします。
- ステップ 4 ローカルユーザアカウントを設定または変更するには、行をクリックします。
- ステップ 5 [User Details] ダイアログボックスで、次のプロパティを更新します。

名前	説明
[Delete Users] ボタン	テーブルにリストされているユーザを削除するには、このボタンをクリックします。

名前	説明
[Enable Strong Pasword] ボタン	強力なパスワードポリシーを有効または無効にするには、このボタンをクリックします。強力なパスワードポリシーを有効にしたら、サーバへの初回ログイン時に、ガイドラインに従い、強力なパスワードを設定する必要があります。ガイドラインを無視して、好きなパスワードを設定する場合は、[Disable Strong Pasword] ボタンをクリックします。デフォルトでは、強力なパスワードポリシーが有効になっています。
[ID] カラム	ユーザの固有識別情報。
[Enabled] チェックボックス	オンにすると、ユーザは CIMC でイネーブルになります。
[Username] カラム	ユーザのユーザ名。
[Role] カラム	ユーザに割り当てられているロール。次のいずれかになります。 <ul style="list-style-type: none"> • [read-only] : 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] : このユーザは次のことが可能です。 <ul style="list-style-type: none"> ◦ 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 • [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 パスワード情報を入力します。

ステップ 7 [Save Changes] をクリックします。

LDAP サーバ (Active Directory)

CIMC では、情報をディレクトリ内で編成してこの情報へのアクセスを管理するディレクトリサービスがサポートされます。CIMC は、ネットワークでディレクトリ情報を保管および保持する Lightweight Directory Access Protocol (LDAP) をサポートします。さらに、CIMC は Microsoft Active

Directory (AD) もサポートします。Active Directory はさまざまなネットワーク サービスを提供するテクノロジーであり、LDAP と同様のディレクトリ サービス、Kerberos ベースの認証、DNS ベースの名前付けなどが含まれます。CIMC は LDAP での Kerberos ベースの認証サービスを利用します。

CIMC で LDAP がイネーブルになっている場合、ローカルユーザデータベース内に見つからないユーザアカウントに関するユーザ認証とロール許可は、LDAP サーバによって実行されます。LDAP ユーザ認証の形式は `username@domain.com` です。

[LDAP Settings] 領域で [Enable Encryption] チェックボックスをオンにすることで、LDAP サーバへの送信データを暗号化するようサーバに要求できます。

LDAP サーバの設定

CIMC を設定して、LDAP をユーザの認証と許可に使用できます。LDAP 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、LDAP スキーマを変更して、属性 ID 1.3.6.1.4.1.9.287247.1 を持つ CiscoAVPair 属性などの新しいカスタム属性を追加できます。



重要 スキーマの変更の詳細については、<http://technet.microsoft.com/en-us/library/bb727064.aspx> の記事を参照してください。



(注) この例では CiscoAVPair という名前のカスタム属性を作成しますが、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。

LDAP サーバに対して次の手順を実行する必要があります。

手順

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

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

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

- ステップ 3** スナップインを使用して、ユーザ クラスに CiscoAVPair 属性を追加します。
- a) 左ペインで [Classes] ノードを展開し、U を入力してユーザ クラスを選択します。
 - b) [Attributes] タブをクリックして、[Add] をクリックします。
 - c) C を入力して CiscoAVPair 属性を選択します。
 - d) [OK] をクリックします。

- ステップ 4** 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> の記事を参照してください。

次の作業

CIMC を使用して LDAP サーバを設定します。

CIMC での LDAP 設定およびグループ許可の設定

はじめる前に

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

手順

- ステップ 1** [Navigation] ペインの [Admin] タブをクリックします。
- ステップ 2** [Admin] タブの [User Management] をクリックします。
- ステップ 3** [User Management] ペインの [Active Directory] タブをクリックします。
- ステップ 4** [LDAP Settings] 領域で、次のプロパティを更新します。

名前	説明
[Enable LDAP] チェックボックス	オンにすると、ユーザ認証とロール許可は、まず LDAP サーバによって実行されてから、ローカル ユーザ データベースに存在しないユーザアカウントによって実行されます。
[Base DN] フィールド	ベース識別名。ユーザとグループのロード元の場所を指定します。 Active Directory サーバの場合、Base DN は dc=domain,dc=com の形式で指定する必要があります。
[Domain] フィールド	IPv4 ドメイン名。すべてのユーザが IPv4 ドメインに存在する必要があります。 グローバル カタログ サーバのアドレスを少なくとも 1 つ指定していない限り、このフィールドは必須です。
[Enable Encryption] チェックボックス	これを選択した場合、サーバは LDAP サーバに送るすべての情報を暗号化します。
[Timeout (0 - 1800) seconds] フィールド	LDAP 検索操作がタイムアウトするまで CIMC が待機する秒数。 検索操作がタイムアウトになった場合、CIMC はこのタブで次にリストされているサーバ（存在する場合）に接続しようと試行します。 (注) このフィールドに指定する値は、全体的な時間に影響を及ぼす可能性があります。

ステップ 5 [Configure LDAP Servers] 領域で、次のプロパティを更新します。

名前	説明
[Pre-Configure LDAP Servers] オプション ボタン	これを選択すると、Active Directory は事前構成された LDAP サーバを使用します。
[LDAP Servers] 領域	

名前	説明
[Server] カラム	<p>6 台の LDAP サーバの IP アドレス。</p> <p>LDAP に Active Directory を使用している場合、サーバ 1、2、3 はドメインコントローラ、サーバ 4、5、6 はグローバルカタログです。LDAP に Active Directory を使用していない場合は、最大 6 台の LDAP サーバを構成できます。</p> <p>(注) また、ホスト名の IP アドレスも提供できます。</p>
[Port] カラム	<p>サーバのポート番号。</p> <p>LDAP に Active Directory を使用している場合、サーバ 1、2、3 (ドメインコントローラ) のデフォルトポート番号は 389 です。サーバ 4、5、6 (グローバルカタログ) のデフォルトポート番号は 3268 です。</p> <p>LDAPS 通信は TCP 636 ポートで発生します。グローバルカタログサーバへの LDAPS 通信は TCP 3269 ポートで発生します。</p>
[Use DNS to Configure LDAP Servers] オプションボタン	<p>これを選択した場合、DNS を使って LDAP サーバへのアクセスを設定できます。</p>
[DNS Parameters] 領域	
[Source] ドロップダウンリスト	<p>DNS SRV 要求に使用されるドメイン名を取得する方法を指定します。次のいずれかになります。</p> <ul style="list-style-type: none"> • [Extracted] : ログイン ID から抽出されるドメインを使用します。 • [Configured] : 設定された検索ドメインを使用します。 • [Configured-Extracted] : 設定された検索ドメインの代わりに、ログイン ID から抽出されるドメイン名を使用します。
[Domain to Search] フィールド	<p>DNS クエリーのソースとして機能する設定済みドメイン名。</p> <p>ソースが [Extracted] と指定される場合、このフィールドは無効になります。</p>

名前	説明
[Forest to Search] フィールド	DNS クエリーのソースとして機能する設定済みフォレスト名。 ソースが [Extracted] と指定される場合、このフィールドは無効になります。

ステップ 6 [Binding Parameters] 領域で、次のプロパティを更新します。

名前	説明
[Method] ドロップダウンリスト	次のいずれかになります。 <ul style="list-style-type: none"> • [Anonymous] : ユーザ名とパスワードを NULL にする必要があります。このオプションを選択し、匿名ログイン用の LDAP サーバを設定している場合、ユーザはアクセスすることができます。 • [Configured Credentials] : 初期バインドプロセスに対して既知のクレデンシャルセットを指定する必要があります。初期バインドプロセスが成功した場合、ユーザ名の Distinguished Name (DN) が照会され、再バインディングプロセス用に再利用されます。再バインディングプロセスが失敗すると、ユーザはアクセスを拒否されます。 • [Login Credentials] : ユーザクレデンシャルが必要です。バインドプロセスが失敗すると、ユーザはアクセスを拒否されます。 (注) [Login Credentials] はデフォルトのオプションです。
[Binding DN] フィールド	ユーザの Distinguished Name (DN) 。 このフィールドは、バインディング方式として [Configured Credentials] オプションを選択した場合にのみ編集可能になります。
[Password] フィールド	ユーザのパスワード。 このフィールドは、バインディング方式として [Configured Credentials] オプションを選択した場合にのみ編集可能になります。

ステップ 7 [Search Parameters] 領域で、次のフィールドを更新します。

名前	説明
[Filter Attribute] フィールド	このフィールドは、LDAP サーバ上のスキーマの設定済み属性に一致する必要があります。 デフォルトでは、このフィールドは [sAMAccountName] と表示されます。
[Group Attribute] フィールド	このフィールドは、LDAP サーバ上のスキーマの設定済み属性に一致する必要があります。 デフォルトでは、このフィールドは [memberOf] と表示されます。
[Attribute] フィールド	ユーザのロールとロケール情報を保持する LDAP 属性。このプロパティは、常に、名前と値のペアで指定されます。システムは、ユーザレコードで、この属性名と一致する値を検索します。 LDAP 属性では、CIMC ユーザ ロールおよびロケールにマップされる既存の LDAP 属性を使用することも、スキーマを変更して新しい LDAP 属性を作成することもできます。（たとえば CiscoAvPair など）。 (注) このプロパティを指定しない場合、ユーザはログインできません。オブジェクトは LDAP サーバ上に存在していますが、このフィールドで指定される属性と正確に一致する必要があります。

ステップ 8 (任意) [Group Authorization] 領域で、次のプロパティを更新します。

名前	説明
[LDAP Group Authorization] チェックボックス	オンにすると、ローカル ユーザ データベース内で検出されなかったユーザ、または Active Directory で CIMC の使用が個別に許可されていないユーザに対するユーザ認証がグループレベルでも実行されます。
[Nested Group Search Depth] フィールド	LDAP グループ マップで定義されている別のグループ内にネストされた LDAP グループを検索するためのパラメータ。このパラメータは、ネストされたグループ検索の深さを定義します。

名前	説明
[Group Name] カラム	サーバへのアクセスが許可されているグループの名前を LDAP データベースに指定します。
[Group Domain] カラム	LDAPサーバのドメインがグループに存在する必要があります。
[Role] カラム	<p>すべてのユーザに割り当てられているこの LDAP サーバグループのロール。次のいずれかになります。</p> <ul style="list-style-type: none"> • [read-only] : 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] : このユーザは次のことが可能です。 <ul style="list-style-type: none"> ◦ 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 • [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 9 [Save Changes] をクリックします。

ユーザセッションの表示

手順

- ステップ 1** [Navigation] ペインの [Admin] タブをクリックします。
- ステップ 2** [Admin] タブの [User Management] をクリックします。
- ステップ 3** [User Management] ペインの [Sessions] タブをクリックします。
- ステップ 4** 現在のユーザセッションに関する次の情報が表示されます。
ヒント カラムの見出しをクリックすると、そのカラムのエントリに従って表の行がソートされます。

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



第 9 章

ネットワーク関連の設定

この章は、次の項で構成されています。

- [CIMC NIC の設定, 141 ページ](#)
- [共通プロパティの設定, 144 ページ](#)
- [IPv4 の設定, 145 ページ](#)
- [VLAN への接続, 146 ページ](#)
- [ネットワークセキュリティの設定, 146 ページ](#)
- [ネットワーク解析機能の有効化, 148 ページ](#)
- [NTP 設定の構成, 148 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

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

- [Dedicated] : CIMC への接続は、管理イーサネット ポートを経由して使用できます。
- Shared LOM : CIMC への接続は、マザーボードのオンボード LAN (LOM) イーサネット ホスト ポート経由およびルータの PCIe と MGF インターフェイス経由で使用できます。



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



(注) 専用モードはEHWIC E シリーズ NCEには適用されません。

NIC 冗長化

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

- [None] : 冗長化は使用できません。
- [Active-Standby] : 1 つのポートから別のポートにフェールオーバーします。

使用できる冗長化モードは、選択されているネットワーク モードとプラットフォームによって異なります。

CIMC NIC の設定

NIC モードと NIC 冗長化を設定するには、次の手順を実行します。

はじめる前に

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

手順

- ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
- ステップ 2 [Admin] タブの [Network] をクリックします。
- ステップ 3 [Network] ペインの [Network Settings] タブをクリックします。
- ステップ 4 [NIC Properties] 領域で、次のプロパティを更新します。

名前	説明
[NIC Mode] ドロップダウン リスト	<p>NIC モード。次のいずれかになります。</p> <ul style="list-style-type: none"> • [Dedicated] : CIMC へのアクセスに管理ポートを使用します。 • [Shared LOM] : CIMC へのアクセスにマザーボードのオンボード LAN (LOM) ポートを使用します。 <p>(注) [Dedicated] モードは、EHWIC E シリーズ NCE および UCS E シリーズ M3 サーバには適用されません。</p>
[NIC Redundancy] ドロップダウン リスト	<p>NIC 冗長性オプションは、[NIC Mode] ドロップダウンリストで選択したモードと、使用しているサーバのモデルによって異なります。あるオプションが表示されない場合、そのオプションは選択されているモードまたはサーバモデルでは使用できません。</p> <p>次のオプションを使用できます。</p> <ul style="list-style-type: none"> • [none] : 設定されている NIC モードに関連付けられた各ポートは個別に動作します。問題が発生した場合、ポートはフェールオーバーしません。 <p>(注) リリース 3.1 以降では、[NIC Redundancy] でサポートされるオプションは [none] だけです。</p> <ul style="list-style-type: none"> • [active-standby] : 設定されている NIC モードに関連付けられたポートで障害が発生した場合、トラフィックは、その NIC モードに関連付けられている他のポートの1つにフェールオーバーします。 <p>(注) このオプションを選択する場合は、設定されている NIC モードに関連付けられたすべてのポートが同じサブネットに接続され、どのポートが使用されてもトラフィックの安全が保証されるようにする必要があります。</p>

名前	説明
[NIC Interface] フィールド	NIC で使用されるインターフェイス。 重要 EHWIC E シリーズ NCE または NIM E シリーズ NCE で外部 GE2 インターフェイスを使用して CIMC アクセスを設定している場合、サーバのリブート中に CIMC との接続が失われることがあります。これは想定されている動作です。リブート中に CIMC との接続を維持する必要がある場合は、他のネットワーク インターフェイスを使用して CIMC アクセスを設定することをお勧めします。『Cisco UCS E シリーズサーバおよび Cisco UCS E シリーズ ネットワーク コンピュート エンジン スタートアップ ガイド』の「CIMC Access Configuration Options—EHWIC E-Series NCE」および「CIMC Access Configuration Options—NIM E-Series NCE」の項を参照してください。
[MAC Address] フィールド	[NIC Mode] フィールドで選択されている CIMC ネットワーク インターフェイスの MAC アドレス。

(注) お使いのプラットフォームによっては、使用できる NIC モード オプションが異なる場合があります。

Shared LOM を選択した場合は、すべてのホスト ポートが同じサブネットに属することを確認してください。

ステップ 5 [Save Changes] をクリックします。

共通プロパティの設定

サーバを説明するには、共通プロパティを使用します。

はじめる前に

共通プロパティを設定するには、admin 権限を持つユーザとしてログインする必要があります。

手順

-
- ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
 - ステップ 2 [Admin] タブの [Network] をクリックします。
 - ステップ 3 [Network] ペインの [Network Settings] タブをクリックします。
 - ステップ 4 [Hostname] フィールドに、ホストの名前を入力します。
 - ステップ 5 [Save Changes] をクリックします。
-

IPv4 の設定

はじめる前に

IPv4 を設定するには、admin 権限を持つユーザとしてログインする必要があります。

手順

-
- ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
 - ステップ 2 [Admin] タブの [Network] をクリックします。
 - ステップ 3 [Network] ペインの [Network Settings] タブをクリックします。
 - ステップ 4 [IPv4 Properties] 領域で、次のプロパティを更新します。

名前	説明
[Enable IPv4] チェックボックス	オンにすると、IPv4 がイネーブルになります。
[Use DHCP] チェックボックス	オンにすると、CIMC は DHCP を使用します。
[IP Address] フィールド	CIMC の IP アドレス。
[Subnet Mask] フィールド	IP アドレスのサブネット マスク。
[Gateway] フィールド	ゲートウェイの IP アドレス。
[Obtain DNS Server Addresses from DHCP] チェックボックス	オンにすると、CIMC は DNS サーバアドレスを DHCP から取得します。
[Preferred DNS Server] フィールド	プライマリ DNS サーバの IP アドレス。
[Alternate DNS Server] フィールド	セカンダリ DNS サーバの IP アドレス。

ステップ 5 [Save Changes] をクリックします。

VLAN への接続

はじめる前に

VLAN に接続するには、admin としてログインしている必要があります。

手順

- ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
- ステップ 2 [Admin] タブの [Network] をクリックします。
- ステップ 3 [Network] ペインの [Network Settings] タブをクリックします。
- ステップ 4 [VLAN Properties] 領域で、次のプロパティを更新します。

名前	説明
[Enable VLAN] チェックボックス	オンにすると、CIMC は仮想 LAN に接続されます。
[VLAN ID] フィールド	VLAN ID。
[Priority] フィールド	VLAN でのこのシステムのプライオリティ。

ステップ 5 [Save Changes] をクリックします。

ネットワーク セキュリティの設定

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、サービス拒絶 (DoS) 攻撃から保護するために使用されます。CIMC は、IP ブロッキングの失敗回数を設定して、IP アドレスを禁止します。

ネットワークセキュリティの設定

IP ブロッキングの失敗回数を設定する場合は、ネットワークセキュリティを設定します。

はじめる前に

ネットワークセキュリティを設定するには、admin 権限を持つユーザとしてログインする必要があります。

手順

- ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
- ステップ 2 [Admin] タブの [Network] をクリックします。
- ステップ 3 [Network] ペインの [Network Security] タブをクリックします。
- ステップ 4 [IP Blocking Properties] 領域で、次のプロパティを更新します。

名前	説明
[Enable IP Blocking] チェックボックス	オンにすると、IP ブロッキングが有効になります。
[IP Blocking Fail Count] フィールド	指定された時間ユーザがロックアウトされる前に、ユーザが試行できるログインの失敗回数。 この回数のログイン試行失敗は、[IP Blocking Fail Window] フィールドで指定されている期間内に発生する必要があります。 3 ~ 10 の範囲の整数を入力します。
[IP Blocking Fail Window] フィールド	ユーザをロックアウトするためにログイン試行の失敗が発生する必要がある期間 (秒数)。 60 ~ 120 の範囲の整数を入力します。
[IP Blocking Penalty Time] フィールド	ユーザが指定されている期間内にログイン試行の最大回数を超えた場合に、ユーザがロックアウトされている秒数。 300 ~ 900 の範囲の整数を入力します。

- ステップ 5 [Save Changes] をクリックします。

ネットワーク解析機能の有効化

はじめる前に

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

手順

- ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
- ステップ 2 [Admin] タブの [Network] をクリックします。
- ステップ 3 [Network] ペインの [Network Analysis] タブをクリックします。
- ステップ 4 [Network Analysis Capability] 領域で、[Enabled] チェックボックスをオンにします。ルータに、ネットワーク解析モジュール (NAM) 機能をオンにする通知が届きます。
- ステップ 5 [Save Changes] をクリックします。

NTP 設定の構成

NTP 設定

デフォルトでは、CIMC がリセットされると、ホストと時刻が同期されます。Network Time Protocol (NTP) サービスを導入すると、CIMC を設定して NTP サーバと時刻を同期できます。デフォルトでは、NTP サーバは CIMC で動作しません。NTP サーバまたは時刻源サーバとして機能するサーバ (少なくとも 1 台、最大 4 台) の IP アドレスまたは DNS アドレスを指定し、NTP サービスをイネーブルにして設定する必要があります。NTP サービスをイネーブルにすると、CIMC は設定された NTP サーバと時刻を同期します。NTP サービスは CIMC でのみ変更できます。



- (注) NTP サービスをイネーブルにするには、DNS アドレスではなく、サーバの IP アドレスを指定することを推奨します。

NTP 設定の構成

NTP を設定すると、IPMI の Set SEL time コマンドはディセーブルになります。

はじめる前に

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

手順

- ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
- ステップ 2 [Admin] タブの [Network] をクリックします。
- ステップ 3 [Network] ペインの [NTP Settings] タブをクリックします。
- ステップ 4 [NTP Settings] 領域で、次のプロパティを更新します。

名前	説明
[Enable NTP] チェックボックス	オンにすると、NTP サービスが有効になります。
サーバ 1	NTP サーバまたは時刻源サーバとして機能する 4 台のサーバのうちの 1 台の IP アドレスまたはドメイン名。
サーバ 2	NTP サーバまたは時刻源サーバとして機能する 4 台のサーバのうちの 1 台の IP アドレスまたはドメイン名。
サーバ 3	NTP サーバまたは時刻源サーバとして機能する 4 台のサーバのうちの 1 台の IP アドレスまたはドメイン名。
サーバ 4	NTP サーバまたは時刻源サーバとして機能する 4 台のサーバのうちの 1 台の IP アドレスまたはドメイン名。

- ステップ 5 [Save Changes] をクリックします。



第 10 章

コミュニケーションサービスの設定

この章は、次の項で構成されています。

- [HTTP の設定, 151 ページ](#)
- [SSH の設定, 152 ページ](#)
- [XML API の設定, 153 ページ](#)
- [IPMI の設定, 154 ページ](#)
- [SNMP の設定, 156 ページ](#)

HTTP の設定

はじめる前に

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

手順

- ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
- ステップ 2 [Admin] タブの [Communications Services] をクリックします。
- ステップ 3 [Communications Services] ペインの [Communication Services] タブをクリックします。
- ステップ 4 [HTTP Properties] 領域で、次のプロパティを更新します。

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

名前	説明
[Redirect HTTP to HTTPS Enabled] チェックボックス	イネーブルの場合、HTTP 経由で試行される通信はすべて同等の HTTPS アドレスにリダイレクトされます。 HTTP をイネーブルにしている場合は、このオプションをイネーブルにすることを強く推奨します。
[HTTP Port] フィールド	HTTP 通信に使用するポート。デフォルトは 80 です。
[HTTPS Port] フィールド	HTTPS 通信に使用するポート。デフォルトは 443 です。
[Session Timeout] フィールド	HTTP 要求の間、CIMC がタイムアウトしてセッションを終了するまで待機する秒数。 60 ~ 10,800 の範囲の整数を入力します。デフォルトは 1,800 秒です。
[Max Sessions] フィールド	CIMC で許可されている HTTP および HTTPS の同時セッションの最大数。 この値は変更できません。
[Active Sessions] フィールド	CIMC で現在実行されている HTTP および HTTPS セッションの数。

ステップ 5 [Save Changes] をクリックします。

SSH の設定

はじめる前に

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

手順

- ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
- ステップ 2 [Admin] タブの [Communications Services] をクリックします。
- ステップ 3 [Communications Services] ペインの [Communication Services] タブをクリックします。
- ステップ 4 [SSH Properties] 領域で、次のプロパティを更新します。

名前	説明
[SSH Enabled] チェックボックス	SSH が CIMC でイネーブルかディセーブルか。
[SSH Port] フィールド	セキュア シェル アクセスに使用するポート。デフォルトは 22 です。
[SSH Timeout] フィールド	SSH 要求がタイムアウトしたものとシステムが判断するまで待機する秒数。 60 ~ 10,800 の範囲の整数を入力します。デフォルトは 1,800 秒です。
[Max Sessions] フィールド	CIMC で許可されている SSH の同時セッションの最大数。 この値は変更できません。
[Active Sessions] フィールド	CIMC で現在実行されている SSH セッションの数。

ステップ 5 [Save Changes] をクリックします。

XML API の設定

CIMC の XML API

Cisco CIMC XML Application Programming Interface (API) は、E シリーズ サーバ 対応の CIMC に対するプログラマチック インターフェイスです。この API は、HTTP または HTTPS 経由で XML ドキュメントを受け取ります。

XML API に関する詳細については、『*CIMC XML API Programmer's Guide for Cisco UCS E-Series Servers*』を参照してください。

XML API のイネーブル化

はじめる前に

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

手順

- ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
- ステップ 2 [Admin] タブの [Communications Services] をクリックします。
- ステップ 3 [Communications Services] ペインの [Communication Services] タブをクリックします。
- ステップ 4 [XML API Properties] 領域で、次のプロパティを更新します。

名前	説明
[XML API Enabled] チェックボックス	このサーバで API アクセスが許可されているかどうか。
[Max Sessions] フィールド	CIMC で許可されている API の同時セッションの最大数。 この値は変更できません。
[Active Sessions] フィールド	現在 CIMC で実行されている API セッションの数。

- ステップ 5 [Save Changes] をクリックします。

IPMI の設定

IPMI over LAN

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

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

IPMI over LAN の設定

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

はじめる前に

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

手順

- ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
- ステップ 2 [Admin] タブの [Communications Services] をクリックします。
- ステップ 3 [Communications Services] ペインの [Communication Services] タブをクリックします。
- ステップ 4 [IPMI over LAN Properties] 領域で、次のプロパティを更新します。

名前	説明
[Enabled] チェックボックス	このサーバで IPMI アクセスが許可されているかどうか。
[Privilege Level Limit] ドロップダウンリスト	このサーバで IPMI セッションに割り当て可能な最高特権レベル。次のいずれかになります。 <ul style="list-style-type: none"> • [read-only] : IPMI ユーザは情報を表示できますが、変更することはできません。このオプションを選択した場合、「Administrator」、「Operator」、または「User」ユーザロールを持つ IPMI ユーザが作成できるのは、読み取り専用の IPMI セッションだけです。それ以外に所持している IPMI 特権は関係ありません。 • [user] : IPMI ユーザはいくつかの機能を実行できますが、管理タスクは実行できません。このオプションを選択した場合、「Administrator」または「Operator」ユーザロールを持つ IPMI ユーザがこのサーバで作成できるのは、ユーザセッションと読み取り専用セッションだけです。 • [admin] : IPMI ユーザは使用可能なすべてのアクションを実行できます。このオプションを選択した場合、「Administrator」ユーザロールを持つ IPMI ユーザは、管理者、ユーザ、および読み取り専用セッションをこのサーバで作成できます。
[Encryption Key] フィールド	IPMI 通信に使用する IPMI 暗号キー。

- ステップ 5 [Save Changes] をクリックします。

SNMP の設定

SNMP

Cisco UCS E-Series Servers は、サーバの設定およびステータスを表示したり、SNMP トラップによって障害とアラートを送信したりするために、簡易ネットワーク管理プロトコル (SNMP) をサポートしています。CIMC でサポートされている Management Information Base (MIB) ファイルの詳細については、次の URL にある『*MIB Quick Reference for Cisco UCS*』を参照してください。
http://www.cisco.com/en/US/docs/unified_computing/ucs/sw/mib/reference/UCS_MIBRef.html

SNMP プロパティの設定

はじめる前に

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

手順

- ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
- ステップ 2 [Admin] タブの [Communications Services] をクリックします。
- ステップ 3 [Communications Services] ペインの [SNMP] タブをクリックします。
- ステップ 4 [SNMP Properties] 領域で、次のプロパティを更新します。

名前	説明
[SNMP Enabled] チェックボックス	このサーバが指定のホストに SNMP トラップを送信するかどうか。 (注) このチェックボックスをオンにしたら、SNMP ユーザまたはトラップを設定する前に、[Save Changes] をクリックする必要があります。
[SNMP Port] フィールド	サーバが SNMP ホストとの通信に使用するポート。 この値は変更できません。
[Access Community String] フィールド	CIMC が SNMP ホストに送信するトラップメッセージに含まれるデフォルトの SNMP v1 または v2c コミュニティ名あるいは SNMP v3 ユーザ名。 最大 18 文字の文字列を入力します。

名前	説明
[SNMP Community Access] ドロップダウン リスト	次のいずれかになります。 <ul style="list-style-type: none"> • [Disabled] : このオプションは、インベントリ テーブルの情報へのアクセスをブロックします。 • [Limited] : このオプションは、インベントリ テーブルの情報への部分的な読み取りアクセスを提供します。 • [Full] : このオプションは、インベントリ テーブルの情報へのフル読み取りアクセスを提供します。
[Trap Community String] フィールド	トラップ情報の送信先となる SNMP コミュニティグループの名前。 最大 18 文字の文字列を入力します。
[System Contact] フィールド	SNMP の実装を担当するシステムの連絡先。 電子メール アドレスまたは名前と電話番号など、最大 64 文字の文字列を入力します。
[System Location] フィールド	SNMP エージェント（サーバ）が実行するホストの場所。 最大 64 文字の文字列を入力します。
[SNMP Engine ID] フィールド	SNMP エンジンの ID。

ステップ 5 [Save Changes] をクリックします。

次の作業

「[SNMP トラップ設定の指定](#), (157 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

プラットフォーム イベント アラートをディセーブルにするには、admin 権限を持つユーザとしてログインする必要があります。

手順

- ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
- ステップ 2 [Admin] タブの [Communications Services] をクリックします。
- ステップ 3 [Communications Services] ペインの [SNMP] タブをクリックします。
- ステップ 4 [Trap Destinations] タブをクリックします。
- ステップ 5 [Trap Destinations] 領域で、次のいずれかを実行できます。
- トラップの宛先情報を変更する場合は、有効になっている行を選択して [Modify] をクリックします。
 - 新しいトラップの宛先を設定する場合は、行を選択して [Add] をクリックします。

(注) フィールドが強調表示されていない場合は、[Enabled] を選択します。

ステップ 6 [Trap Details] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[ID] フィールド	トラップの宛先 ID。この値は変更できません。
[Enabled] チェックボックス	オンにすると、このトラップがサーバでアクティブになります。
[System Version] ドロップダウンリスト	トラップに使用される SNMP バージョンおよびモデル。次のいずれかになります。 <ul style="list-style-type: none"> • V2 • V3
[Trap Type] オプション ボタン	バージョンに [V2] を選択した場合、これが送信するトラップのタイプになります。次のいずれかになります。 <ul style="list-style-type: none"> • [Trap] : このオプションを選択すると、トラップが宛先に送信されますが、通知は受信しません。 • [Inform] : このオプションを選択すると、トラップが宛先で受信されたときに通知を受信します。
[User] ドロップダウン リスト	ドロップダウンリストに使用可能なすべてのユーザが表示されます。そのリストからユーザを選択します。
[Trap Destination Adress] フィールド	SNMP トラップ情報の送信先の IP アドレス。

名前	説明
Port	サーバがトラップの宛先との通信に使用するポート。1～65535の範囲内のトラップの宛先のポート番号を入力します。

ステップ 7 [Save Changes] をクリックします。

ステップ 8 トラップの宛先を削除する場合は、その行を選択して [Delete] をクリックします。確認のプロンプトで [OK] をクリックします。

SNMP テストトラップメッセージの送信

はじめる前に

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

手順

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

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

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

ステップ 4 [SNMP] タブをクリックし、[Trap Destinations] タブをクリックします。

ステップ 5 [Trap Destinations] 領域で、目的の SNMP トラップ宛先の行を選択します。

ステップ 6 [Send SNMP Test Trap] をクリックします。

SNMP テストトラップメッセージがトラップ宛先に送信されます。

(注) テストメッセージを送信するために、トラップは設定済みで、イネーブルにされている必要があります。

SNMP ユーザの設定

はじめる前に

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

手順

- ステップ 1** [Navigation] ペインの [Admin] タブをクリックします。
- ステップ 2** [Admin] タブの [Communications Services] をクリックします。
- ステップ 3** [Communications Services] ペインの [SNMP] タブをクリックします。
- ステップ 4** SNMP を有効にします（有効ではない場合）。[SNMP Properties] 領域で [SNMP Enabled] チェックボックスをオンして、[Save Changes] をクリックします。
- ステップ 5** [Users] 領域の [User Settings] タブで、次のいずれかを実行します。
- テーブルから既存のユーザを選択し、[Modify] をクリックします。
 - [Add] をクリックして新しいユーザを作成します。[SNMP User Details] ダイアログボックスが表示されます。
- ステップ 6** 次のプロパティを更新します。

名前	説明
[ID] フィールド	ユーザの固有識別情報。このフィールドは変更できません。
[Name] フィールド	SNMP ユーザ名。
[Security Level] ドロップダウンリスト	このユーザのセキュリティレベル。次のいずれかになります。 <ul style="list-style-type: none"> • [no auth, no priv] : このユーザには、許可パスワードもプライバシーパスワードも不要です。 • [auth, no priv] : このユーザには、許可パスワードが必要ですが、プライバシーパスワードは不要です。このオプションを選択すると、CIMCは後述の Auth フィールドをイネーブルにします。 • [auth, priv] : このユーザには、許可パスワードとプライバシーパスワードの両方が必要です。このオプションを選択すると、CIMCは Auth フィールドおよび Privacy フィールドをイネーブルにします。
[Auth Type] フィールド	許可タイプ。次のいずれかになります。 <ul style="list-style-type: none"> • MD5 • SHA
[Auth Password] フィールド	この SNMP ユーザの許可パスワード。
[Confirm Auth Password] フィールド	確認のための許可パスワードの再入力。

名前	説明
[Privacy Type] フィールド	プライバシー タイプ。次のいずれかになります。 <ul style="list-style-type: none"> • DES • AES
[Privacy Password] フィールド	この SNMP ユーザのプライバシー パスワード。
[Confirm Privacy Password] フィールド	確認のための許可パスワードの再入力。

ステップ 7 [Save Changes] をクリックします。

ステップ 8 ユーザを削除する場合は、ユーザを選択し、[Delete] をクリックします。削除の確認プロンプトで、[OK] をクリックします。

SNMP ユーザの管理

はじめる前に

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

手順

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

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

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

ステップ 4 [Users] 領域の [User Settings] タブで、次のプロパティを更新します。

名前	説明
[Add] ボタン	テーブル内で使用できる行をクリックし、このボタンをクリックして新規の SNMP ユーザを追加します。
[Modify] ボタン	テーブル内で変更するユーザを選択し、このボタンをクリックして、選択した SNMP ユーザを変更します。
[Delete] ボタン	テーブル内で削除するユーザを選択し、このボタンをクリックして、選択した SNMP ユーザを削除します。

名前	説明
[ID] カラム	SNMP ユーザに対してシステムが割り当てる識別子。
[Name] カラム	SNMP ユーザ名。
[Auth Type] カラム	ユーザ認証タイプ。
[Privacy Type] カラム	ユーザ プライバシー タイプ。

ステップ 5 [Save Changes] をクリックします。



第 11 章

証明書管理

この章は、次の項で構成されています。

- [サーバ証明書の管理, 163 ページ](#)
- [証明書署名要求の生成, 164 ページ](#)
- [自己署名証明書の作成, 165 ページ](#)
- [サーバ証明書のアップロード, 167 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認証局（CA）、または独自に使用している認証局のいずれかによって署名されます。

手順

- ステップ 1** CIMC から CSR を生成します。
 - ステップ 2** 証明書の発行と署名を行う認証局に CSR ファイルを送信します。組織で独自の自己署名証明書を生成している場合は、CSR ファイルを使用して自己署名証明書を生成できます。
 - ステップ 3** 新しい証明書を CIMC にアップロードします。
(注) アップロードされた証明書は、CIMC によって生成された CSR から作成される必要があります。この方法で作成されていない証明書はアップロードしないでください。
-

証明書署名要求の生成

はじめる前に

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

手順

- ステップ 1** [Navigation] ペインの [Admin] タブをクリックします。
- ステップ 2** [Admin] タブの [Certificate Management] をクリックします。
- ステップ 3** [Actions] 領域で、[Generate New Certificate Signing Request] リンクをクリックします。
[Generate New Certificate Signing Request] ダイアログボックスが表示されます。
- ステップ 4** [Generate New Certificate Signing Request] ダイアログボックスで、次のプロパティを更新します。

名前	説明
[Common Name] フィールド	CIMC の完全修飾ホスト名
[Organization Name] フィールド	証明書を要求している組織。
[Organization Unit] フィールド	組織ユニット
[Locality] フィールド	証明書を要求している会社の本社が存在する市または町。
[State Name] フィールド	証明書を要求している会社の本社が存在する州または行政区分。
[Country Code] ドロップダウンリスト	会社が存在する国。
[Email] フィールド	会社の電子メールによる連絡先。

- ステップ 5** [Generate CSR] をクリックします。
[Opening csr.txt] ダイアログボックスが表示されます。
- ステップ 6** CSR ファイル csr.txt を管理するには、次のいずれかの手順を実行します。
- [Open With] をクリックして csr.txt を表示します。
 - [Save File] をクリックしてから [OK] をクリックし、ローカルマシンに csr.txt を保存します。

次の作業

証明書の発行と署名を行う認証局に CSR ファイルを送信します。組織で独自の自己署名証明書を生成している場合は、CSR ファイルを使用して自己署名証明書を生成できます。

自己署名証明書の作成

パブリック認証局 (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> 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： <pre># openssl genrsa -out ca.key 1024</pre>	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： <pre># openssl req -new -x509 -days 365 -key ca.key -out ca.crt</pre>	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： <pre># echo "nsCertType = server" > openssl.conf</pre>	このコマンドは、証明書がサーバ限定の証明書であることを指定する行を OpenSSL 設定ファイルに追加します。この指定により、認証されたクライアントがサーバになります。man-in-the-middle 攻撃を防御できます。 OpenSSL 設定ファイル openssl.conf には、"nsCertType = server" という文が含まれています。

	コマンドまたはアクション	目的
ステップ 4	<pre>openssl x509 -req -days numdays -in CSR_filename -CA CA_certfilename -set_serial 04 -CAkey CA_keyfilename -out server_certfilename -extfile openssl.conf</pre> <p>例 :</p> <pre># openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 04 -CAkey ca.key -out myserver05.crt -extfile openssl.conf</pre>	<p>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。</p> <p>サーバ証明書は、出力ファイルに含まれていません。</p>

この例は、CA の作成方法、および新規に作成された CA が署名するサーバ証明書の生成方法を示します。これらのコマンドは、OpenSSL を実行している Linux サーバで入力します。

```
# /usr/bin/openssl genrsa -out ca.key 1024
Generating RSA private key, 1024 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)
# /usr/bin/openssl req -new -x509 -days 365 -key ca.key -out ca.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:California
Locality Name (eg, city) [Newbury]:San Jose
Organization Name (eg, company) [My Company Ltd]:Example Incorporated
Organizational Unit Name (eg, section) []:Unit A
Common Name (eg, your name or your server's hostname) []:example.com
Email Address []:admin@example.com
# echo "nsCertType = server" > openssl.conf
# /usr/bin/openssl x509 -req -days 365 -in csr.txt -CA ca.crt -set_serial 01 -CAkey ca.key -out server.crt
-extfile openssl.conf
Signature ok
subject=/C=US/ST=California/L=San Jose/O=Example Inc./OU=Unit
A/CN=example.com/emailAddress=john@example.com
Getting CA Private Key
#
```

次の作業

新しい証明書を CIMC にアップロードします。

サーバ証明書のアップロード

はじめる前に

証明書をアップロードするには、admin 権限を持つユーザとしてログインする必要があります。アップロードする証明書ファイルは、ローカルにアクセスできるファイルシステムに配置されている必要があります。



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

手順

- ステップ 1** [Navigation] ペインの [Admin] タブをクリックします。
- ステップ 2** [Admin] タブの [Certificate Management] をクリックします。
- ステップ 3** [Actions] 領域で、[Upload Server Certificate] をクリックします。
[Upload Certificate] ダイアログボックスが表示されます。
- ステップ 4** [Upload Certificate] ダイアログボックスで、次のプロパティを更新します。

名前	説明
[File] フィールド	アップロードする証明書ファイル。
[Browse] ボタン	適切な証明書ファイルに移動できるダイアログボックスが表示されます。 注意 [Browse] ボタンを使用して証明書ファイルを選択した後は、キーボードの Backspace ボタンを使用して証明書ファイル名を編集しないでください。編集すると、CIMC からログアウトされます。

- ステップ 5** [Upload Certificate] をクリックします。



第 12 章

プラットフォームイベントフィルタの設定

この章は、次の項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, 169 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, 169 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, 170 ページ](#)
- [プラットフォーム イベント フィルタの設定, 170 ページ](#)
- [プラットフォーム イベント トラップの解釈, 171 ページ](#)

プラットフォーム イベント フィルタ

プラットフォーム イベント フィルタ (PEF) は、ハードウェア関連の重要なイベントが発生したときに、アクションをトリガーしたりアラートを生成したりできます。PEF ごとに、プラットフォーム イベントが発生したときに実行するアクション (またはアクションを実行しないこと) を選択できます。また、プラットフォーム イベントが発生したときにアラートを生成して送信することもできます。アラートは SNMP トラップとして送信されるので、アラートを送信するには、先に SNMP トラップの宛先を設定する必要があります。

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

プラットフォーム イベント アラートのイネーブル化

はじめる前に

プラットフォーム イベント アラートをイネーブルにするには、admin 権限を持つユーザとしてログインする必要があります。

手順

-
- ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
 - ステップ 2 [Admin] タブの [Event Management] をクリックします。
 - ステップ 3 [Event Management] ペインの [Platform Event Filters] タブをクリックします。
 - ステップ 4 [Platform Event Alerts] 領域で、[Enable Platform Event Alerts] チェックボックスをオンにします。
 - ステップ 5 [Save Changes] をクリックします。
-

プラットフォーム イベント アラートのディセーブル化

はじめる前に

プラットフォーム イベント アラートをディセーブルにするには、admin 権限を持つユーザとしてログインする必要があります。

手順

-
- ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
 - ステップ 2 [Admin] タブの [Event Management] をクリックします。
 - ステップ 3 [Event Management] ペインの [Platform Event Filters] タブをクリックします。
 - ステップ 4 [Platform Event Alerts] 領域で、[Enable Platform Event Alerts] チェックボックスをオフにします。
 - ステップ 5 [Save Changes] をクリックします。
-

プラットフォーム イベント フィルタの設定

はじめる前に

プラットフォーム イベント フィルタを設定するには、admin 権限を持つユーザとしてログインする必要があります。

手順

- ステップ 1** [Navigation] ペインの [Admin] タブをクリックします。
- ステップ 2** [Admin] タブの [Event Management] をクリックします。
- ステップ 3** [Event Management] ペインの [Platform Event Filters] タブをクリックします。
- ステップ 4** [Platform Event Filters] 領域で、各イベントの次のフィールドに入力します。

名前	説明
[ID] カラム	一意のフィルタ ID。
[Event] カラム	イベント フィルタの名前。
[Action] カラム	フィルタごとに、目的の処理をスクロールリストボックスから選択します。次のいずれかになります。 <ul style="list-style-type: none"> • [None] : アクションが実行されません。 • [Reboot] : サーバがリブートされます。 • [Power Cycle] : サーバの電源が再投入されます。 • [Power Off] : サーバの電源がオフになります。
[Send Alert] カラム	アラートを送信するフィルタごとに、このカラムの対応するチェックボックスを選択します。 (注) アラートを送信するには、フィルタ トラップの設定を正しく設定し、[Enable Platform Event Filters] チェックボックスもオンにする必要があります。

- ステップ 5** [Save Changes] をクリックします。

次の作業

PEF を設定してアラートを送信する場合は、次のタスクを完了させます。

- [プラットフォーム イベント アラートのイネーブル化](#), (169 ページ)

プラットフォーム イベント トラップの解釈

SNMP トラップとして送信された CIMC プラットフォーム イベント アラートには、エンタープライズ オブジェクト ID (OID) が `1.3.6.1.4.1.3183.1.1.0.event` の形式で含まれています。OID の最初の 10 個のフィールドは、

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).wired_for_management(3183).PET(1).version(1).version(0) を表し、IPMI プラットフォーム イベントトラップ (PET) バージョン 1.0 メッセージであることを示しています。最後のフィールドはイベント番号であり、通知されている特定の状態またはアラートを示しています。

プラットフォーム イベントトラップの説明

次の表に、プラットフォーム イベントトラップ メッセージで通知されるイベントの説明を示します。これらは、トラップ OID のイベント番号に基づいています。

イベント番号 [注記 1]	プラットフォーム イベントの説明	
0	0h	テストトラップ
65799	010107h	温度に関する警告
65801	010109h	温度が重大な状態
131330	020102h	電圧不足、緊急
131337	020109h	電圧が重大な状態
196871	030107h	電流に関する警告
262402	040102h	ファンが重大な状態
459776	070400h	プロセッサ関連 (IOH-Thermalert/Caterr センサー) : 予測障害非アサート
459777	070401h	プロセッサ関連 (IOH-Thermalert/Caterr センサー) : 予測障害アサート
460032	070500h	プロセッサ電力警告: 制限未超過
460033	070501h	プロセッサ電力警告: 制限超過
524533	0800F5h	電源が重大な状態
524551	080107h	電源に関する警告
525313	080401h	個々の電源に関する警告
527105	080B01h	電源冗長性の損失
527106	080B02h	電源冗長性復元
552704	086F00h	電源挿入済み
552705	086F01h	電源モジュール障害
552707	086F03h	電源 AC の損失
786433	0C0001h	修正可能な ECC メモリ エラー、リリース 1.3(1) 以降のリリース、すべての読み取りタイプを受け入れるように設定されたフィルタ [注記 4]

イベント番号 [注記 1]		プラットフォーム イベントの説明
786439	0C0007h	DDR3_INFO センサー LED : RED ビットアサート (DIMM での ECC エラーの可能性が高い)、汎用センサー [注記 2、3] (注) E シリーズ サーバおよび SM E シリーズ NCE に表示されます。EHWIC E シリーズ NCE および NIM E シリーズ NCE には表示されません。
786689	0C0101h	修正可能な ECC メモリ エラー、リリース 1.3(1) 以降のリリース
818945	0C7F01h	修正可能な ECC メモリ エラー、リリース 1.2(x) 以前のリリース
818951	0C7F07h	DDR3_INFO センサー LED : RED ビットアサート (DIMM での ECC エラーの可能性が高い)、1.2(x) 以前のリリース [注記 3] (注) E シリーズ サーバおよび SM E シリーズ NCE に表示されます。EHWIC E シリーズ NCE および NIM E シリーズ NCE には表示されません。
851968	0D0000h	HDD センサーで障害が示されない、汎用センサー [注記 2]
851972	0D0004h	HDD センサーで障害が示される、汎用センサー [注記 2]
854016	0D0800h	HDD が存在しない、汎用センサー [注記 2]
854017	0D0801h	HDD が存在する、汎用センサー [注記 2]
880384	0D6F00h	HDD あり、障害の兆候なし
880385	0D6F01h	HDD の障害
880512	0D6F80h	HDD が存在しない
880513	0D6F81h	HDD がアサート解除されたが障害状態ではない
884480	0D7F00h	ドライブ スロット LED オフ
884481	0D7F01h	ドライブ スロット LED オン
884482	0D7F02h	ドライブ スロット LED 高速で点滅
884483	0D7F03h	ドライブ スロット LED 低速で点滅
884484	0D7F04h	ドライブ スロット LED 緑
884485	0D7F05h	ドライブ スロット LED オレンジ
884486	0D7F01h	ドライブ スロット LED 青
884487	0D7F01h	ドライブ スロット LED 読み取り
884488	0D7F08h	ドライブ スロット オンライン
884489	0D7F09h	ドライブ スロット 低下

イベント番号 [注記 1]	プラットフォーム イベントの説明
(注)	すべての読み取りタイプを受け入れるようにイベントフィルタが設定された場合は、16進のイベント番号のビット 15:8 は 0 にマスクされます。たとえば、イベント番号 786689 (0C0101h) は 786433 (0C0001h) になります。



第 13 章

ファームウェア管理

この章は、次の項で構成されています。

- [ファームウェアの概要, 175 ページ](#)
- [ファームウェアのアップグレードのオプション, 176 ページ](#)
- [シスコからのソフトウェアの取得, 177 ページ](#)
- [リモートサーバからの CIMC ファームウェアのインストール, 178 ページ](#)
- [ブラウザ経由の CIMC ファームウェアのインストール, 180 ページ](#)
- [インストールした CIMC ファームウェアのアクティブ化, 181 ページ](#)
- [ブラウザ経由の BIOS ファームウェアのインストール, 182 ページ](#)
- [TFTP サーバからの BIOS ファームウェアのインストール, 183 ページ](#)

ファームウェアの概要

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

潜在的な問題を回避するには、Host Upgrade Utility (HUU) を使用することを強く推奨します。このユーティリティは、CIMC、BIOS、およびその他のファームウェア コンポーネントを互換性のあるレベルにアップグレードします。このユーティリティの詳細については、*Cisco UCS E* シリーズサーバおよび *Cisco UCS E* シリーズ ネットワーク コンピュート エンジン スタートアップ ガイドの「Upgrading Firmware」の章を参照してください。この章には、互換性のある HUU、CIMC、および BIOS ソフトウェア リリースに関する情報も含まれています。



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

HUU を使用する代わりに CIMC および BIOS ファームウェアを手動でアップグレードする場合、まず CIMC ファームウェアを更新してから、BIOS ファームウェアを更新します。一致する CIMC ファームウェアをアクティブ化するまでは、新しい BIOS ファームウェアをインストールしないでください。インストールすると、サーバがブートしなくなります。

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

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

CIMC ファームウェアをアクティブ化した後は、BIOS ファームウェアを更新できます。サーバは、BIOS アップデート プロセス全体を通して、電源をオフにする必要があります。CIMC がリブートを完了すると、サーバの電源をオンにして、サービスに戻すことができます。



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

ファームウェアのアップグレードのオプション

ファームウェア コンポーネントは、Cisco Host Upgrade Utility (HUU) を使用してアップグレードすることも手動でアップグレードすることもできます。

- HUU：すべてのファームウェア コンポーネントのアップグレードに CIMC および BIOS ファームウェアを含む HUU ISO ファイルを使用することを推奨します。

HUU を使用したファームウェアのアップグレード手順の詳細については、『*Getting Started Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine*』の「Upgrading Firmware」の章を参照してください。



(注) HUU を使用して Programmable Logic Devices (PLD) ファームウェアをアップグレードすることはできません。PLD ファームウェアをアップグレードするには Cisco IOS CLI を使用する必要があります。詳細については、『*CLI Configuration Guide for Cisco UCS E-Series Servers and the Cisco UCS E-Series Network Compute Engine*』の「Upgrading Programmable Logic Devices Firmware on the E-Series EHWIC NCE」の項を参照してください。

- 手動によるアップグレード：BIOS および CIMC のファームウェアを手動でアップグレードするには、シスコからファームウェアを取得し、CIMC GUI または CIMC CLI を使ってアッ

プグレードする必要があります。ファームウェアのアップグレード後、システムを再起動します。

シスコからのソフトウェアの取得

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

手順

- ステップ 1 <http://www.cisco.com/> を参照します。
- ステップ 2 まだログインしていない場合は、ページの右上隅にある [Log In] をクリックし、Cisco.com の資格情報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 [Downloads] (中央) ペインから、[All Downloads] (右下隅) をクリックします。
[Download Software] ページが表示されます。
- ステップ 5 左ペインから、[Products] をクリックします。
- ステップ 6 中央ペインから、[Unified Computing and Servers] をクリックします。
- ステップ 7 右ペインから、[Cisco UCS E-Series Software] をクリックします。
- ステップ 8 右ペインから、ダウンロードするソフトウェアのサーバモデルの名前をクリックします。
[Download Software] ページは次のカテゴリで表示されます。
 - [Unified Computing System (UCSE) Server Drivers] : ドライバが含まれます。
 - [Unified Computing System (UCSE) Server Firmware] : Host Upgrade Utility と BIOS、CIMC、および PLD ファームウェア イメージが含まれます。
 - [Unified Computing System (UCSE) Utilites] : 次の診断イメージが含まれています。
- ステップ 9 適切なソフトウェア カテゴリ リンクをクリックします。
- ステップ 10 ダウンロードするソフトウェア イメージに関連付けられている [Download] ボタンをクリックします。
[End User License Agreement] ダイアログボックスが表示されます。
- ステップ 11 (任意) 複数のソフトウェア イメージをダウンロードするには、次を実行します。
 - a) ダウンロードするソフトウェア イメージに関連付けられている [Add to cart] ボタンをクリックします。
 - b) 右上にある [Download Cart] ボタンをクリックします。
カートに追加したすべてのイメージが表示されます。
 - c) 右下隅にある [Download All] をクリックして、すべてのイメージをダウンロードします。
[End User License Agreement] ダイアログボックスが表示されます。

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

ステップ 13 必要に応じて、次のいずれかを実行します。

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

サーバは、TFTP サーバ上の宛先フォルダに対する読み取り権限を持っていることが必要です。

次の作業

ソフトウェア イメージをインストールします。

リモートサーバからの CIMC ファームウェアのインストール



(注) 潜在的な問題を回避するには、Host Upgrade Utility (HUU) を使用することを強く推奨します。このユーティリティは、CIMC、BIOS、およびその他のファームウェア コンポーネントを互換性のあるレベルにアップグレードします。このユーティリティの詳細については、*Cisco UCS E* シリーズ サーバおよび *Cisco UCS E* シリーズ ネットワーク コンピュータ エンジン スタートアップ ガイドの「Upgrading Firmware」の章を参照してください。この章には、互換性のある HUU、CIMC、および BIOS ソフトウェア リリースに関する情報も含まれています。

HUU を使用する代わりに CIMC および BIOS ファームウェアを手動でアップグレードする場合、まず CIMC ファームウェアを更新してから、BIOS ファームウェアを更新します。一致する CIMC ファームウェアをアクティブ化するまでは、新しい BIOS ファームウェアをインストールしないでください。インストールすると、サーバがブートしなくなります。

はじめる前に

- ブラウザ経由で CIMC ファームウェアをインストールするには、admin 権限を持つユーザとしてログインする必要があります。
- シスコから CIMC ファームウェア ファイルを取得します。 [シスコからのソフトウェアの取得](#)、(177 ページ) を参照してください。
- TFTP、FTP、SFTP、SCP、HTTP などのリモートサーバで、適切な .bin アップグレード ファイルを解凍します。

手順

- ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
- ステップ 2 [Admin] タブの [Firmware Management] をクリックします。
- ステップ 3 [Actions] 領域で、[Install CIMC Firmware from Remote Server] をクリックします。
- ステップ 4 [Install CIMC Firmware] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Install CIMC Firmware from] ドロップダウン リスト	<p>ファームウェア イメージが配置されているリモートサーバのタイプ。次のいずれかになります。</p> <ul style="list-style-type: none"> • TFTP サーバ • FTP サーバ • [SFTP Server] • SCP サーバ • HTTP サーバ <p>(注) ドロップダウンリストから選択するリモートサーバによって、表示されるフィールドが変わります。</p>
[TFTP]、[FTP]、[SFTP]、[SCP]、または [HTTP Server IP/Hostname] フィールド	<p>ファームウェア イメージが存在するサーバの IP アドレスまたはホスト名。</p>
[Image Path and Filename] フィールド	<p>ファームウェア イメージのパスとファイル名。</p> <p>ファイル名を入力する場合は、サーバツリーの最上位からファイルの場所までのイメージファイルの相対パスを含めてください。</p>
[Username] フィールド	<p>システムがリモートサーバへのログインに使用する必要のあるユーザ名。</p> <p>(注) ユーザ名を設定しない場合は、ユーザ名として anonymous を入力し、パスワードとして任意の文字を入力します。</p> <p>(注) このフィールドは、リモートサーバが TFTP または HTTP の場合は表示されません。</p>

名前	説明
[Password] フィールド	<p>リモート サーバのユーザ名のパスワード。</p> <p>(注) ユーザ名を設定しない場合は、ユーザ名として <code>anonymous</code> を入力し、パスワードとして任意の文字を入力します。</p> <p>(注) このフィールドは、リモート サーバが TFTP または HTTP の場合は表示されません。</p>

ステップ 5 [Install Firmware] をクリックします。

次の作業

CIMC ファームウェアをアクティブにします。

ブラウザ経由の CIMC ファームウェアのインストール



(注) 潜在的な問題を回避するには、Host Upgrade Utility (HUU) を使用することを強く推奨します。このユーティリティーは、CIMC、BIOS、およびその他のファームウェアコンポーネントを互換性のあるレベルにアップグレードします。このユーティリティーの詳細については、*Cisco UCS E* シリーズ サーバおよび *Cisco UCS E* シリーズ ネットワーク コンピュート エンジン スタートアップ ガイドの「Upgrading Firmware」の章を参照してください。この章には、互換性のある HUU、CIMC、および BIOS ソフトウェア リリースに関する情報も含まれています。

HUU を使用する代わりに CIMC および BIOS ファームウェアを手動でアップグレードする場合、まず CIMC ファームウェアを更新してから、BIOS ファームウェアを更新します。一致する CIMC ファームウェアをアクティブ化するまでは、新しい BIOS ファームウェアをインストールしないでください。インストールすると、サーバがブートしなくなります。

はじめる前に

- ブラウザ経由で CIMC ファームウェアをインストールするには、`admin` 権限を持つユーザとしてログインする必要があります。
- シスコから CIMC ファームウェア ファイルを取得します。[シスコからのソフトウェアの取得](#)、(177 ページ) を参照してください。
- ローカル マシンで、適切な `.bin` アップグレード ファイルを解凍します。

手順

-
- ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
 - ステップ 2 [Admin] タブの [Firmware Management] をクリックします。
 - ステップ 3 [Actions] 領域で、[Install CIMC Firmware through Browser Client] をクリックします。
 - ステップ 4 [Install CIMC Firmware] ダイアログボックスで、[Browse] をクリックし、[Choose File] ダイアログボックスを使用して、インストールする .bin ファイルを選択します。
 - ステップ 5 [Install Firmware] をクリックします。
-

次の作業

CIMC ファームウェアをアクティブにします。

インストールした CIMC ファームウェアのアクティブ化

はじめる前に

CIMC ファームウェアをサーバにインストールします。



重要 アクティブ化の進行中は、次のことを行わないでください。

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

手順

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

ブラウザ経由の BIOS ファームウェアのインストール



(注) 潜在的な問題を回避するには、Host Upgrade Utility (HUU) を使用することを強く推奨します。このユーティリティは、CIMC、BIOS、およびその他のファームウェアコンポーネントを互換性のあるレベルにアップグレードします。このユーティリティの詳細については、*Cisco UCS E* シリーズ サーバおよび *Cisco UCS E* シリーズ ネットワーク コンピュート エンジン スタートアップ ガイドの「Upgrading Firmware」の章を参照してください。この章には、互換性のある HUU、CIMC、および BIOS ソフトウェア リリースに関する情報も含まれています。

HUU を使用する代わりに CIMC および BIOS ファームウェアを手動でアップグレードする場合、まず CIMC ファームウェアを更新してから、BIOS ファームウェアを更新します。一致する CIMC ファームウェアをアクティブ化するまでは、新しい BIOS ファームウェアをインストールしないでください。インストールすると、サーバがブートしなくなります。

はじめる前に

- admin 権限を持つユーザとして CIMC にログインします。
- シスコから CIMC ファームウェア ファイルを取得します。 [シスコからのソフトウェアの取得](#)、(177 ページ) を参照してください。
- ローカル マシンで、適切なアップグレード ファイルを解凍します。

手順

- ステップ 1 [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2 [Server] タブの [BIOS] をクリックします。
- ステップ 3 [Firmware Actions] 領域で、[Install BIOS Firmware through Browser Client] をクリックします。
- ステップ 4 [Install BIOS Firmware] ダイアログボックスで、[Browse] をクリックし、[Choose File] ダイアログボックスを使用して、インストールするファイルを選択します。
- ステップ 5 [Install Firmware] をクリックします。
BIOS がダウンロードされ、ホストの電源がオフになり、BIOS がアップグレードされます。アップグレードが完了すると、ホストの電源がオンになります。

TFTP サーバからの BIOS ファームウェアのインストール



(注) 潜在的な問題を回避するには、Host Upgrade Utility (HUU) を使用することを強く推奨します。このユーティリティーは、CIMC、BIOS、およびその他のファームウェアコンポーネントを互換性のあるレベルにアップグレードします。このユーティリティーの詳細については、Cisco UCS E シリーズ サーバおよび Cisco UCS E シリーズ ネットワーク コンピュート エンジン スタートアップガイドの「Upgrading Firmware」の章を参照してください。この章には、互換性のある HUU、CIMC、および BIOS ソフトウェア リリースに関する情報も含まれています。

HUU を使用する代わりに CIMC および BIOS ファームウェアを手動でアップグレードする場合、まず CIMC ファームウェアを更新してから、BIOS ファームウェアを更新します。一致する CIMC ファームウェアをアクティブ化するまでは、新しい BIOS ファームウェアをインストールしないでください。インストールすると、サーバがブートしなくなります。

はじめる前に

- admin 権限を持つユーザとして CIMC にログインします。
- シスコから CIMC ファームウェア ファイルを取得します。[シスコからのソフトウェアの取得](#)、(177 ページ) を参照してください。
- TFTP サーバで、適切なアップグレード ファイルを解凍します。

手順

- ステップ 1 [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2 [Server] タブの [BIOS] をクリックします。
- ステップ 3 [Firmware Actions] 領域で [Install BIOS Firmware from TFTP Server] をクリックします。
- ステップ 4 [Install BIOS Firmware] ダイアログボックスで、次のフィールドに値を入力します。

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

- ステップ 5 [Install Firmware] をクリックします。

BIOS がダウンロードされ、ホストの電源がオフになり、BIOS がアップグレードされます。アップグレードが完了すると、ホストの電源がオンになります。



第 14 章

障害およびログの表示

この章は、次の項で構成されています。

- [障害, 185 ページ](#)
- [システム イベント ログ, 188 ページ](#)
- [Cisco IMC Log, 189 ページ](#)

障害

障害サマリーの表示

手順

- ステップ 1 [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2 [Server] タブの [Faults and Logs] をクリックします。
- ステップ 3 [Faults and Logs] ペインの [Fault Summary] タブをクリックします。
- ステップ 4 [Discrete Sensors] 領域で、次の情報を確認します。

名前	説明
[Sensor Name] カラム	センサーの名前。
[Status] カラム	センサーのステータス。次のいずれかになります。 <ul style="list-style-type: none">• [Critical]• [Non-Recoverable]• [Warning]

名前	説明
[Reading] カラム	次のいずれかになります。 <ul style="list-style-type: none"> • absent • present

ステップ 5 [Threshold Sensors] 領域で、次の情報を確認します。

名前	説明
[Sensor Name] カラム	センサーの名前。
[Status] カラム	センサーのステータス。次のいずれかになります。 <ul style="list-style-type: none"> • [Critical] • [Non-Recoverable] • [Warning]
[Reading] カラム	センサーによって報告される値。
[Units] カラム	センサー データが報告される単位。
[Warning Threshold Min] カラム	Warning の最小しきい値。
[Warning Threshold Max] カラム	Warning の最大しきい値。
[Critical Threshold Min] カラム	Critical の最小しきい値。
[Critical Threshold Max] カラム	Critical の最大しきい値。

障害履歴の表示

手順

- ステップ 1** [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2** [Server] タブの [Faults and Logs] をクリックします。
- ステップ 3** [Faults and Logs] ペインの [Fault History] タブをクリックします。
- ステップ 4** ログの障害イベントごとに次の情報を確認します。

名前	説明
[Timestamp] カラム	障害の発生日時。
[Severity] カラム	障害の重大度。次のいずれかになります。 <ul style="list-style-type: none"> • [Emergency] • [Alert] • [Critical] • [Error] • [Warning] • [Notice] • [Informational] • [Debug]
[Source] カラム	障害をログに記録したソフトウェア モジュール。
[Probable Cause]	障害の原因となったイベントに関連付けられた固有識別情報。
[Description] カラム	障害に関する情報。提案される解決策も含まれます。

- ステップ 5** [Entries Per Page] ドロップダウンリストから、各ページに表示する障害イベントの数を選択します。
- ステップ 6** 障害イベントのページを前方および後方に移動するには [<Newer] および [Older>] をクリックし、リストの先頭に移動するには [<<Newest] をクリックします。デフォルトでは、最新の障害イベントがリストの先頭に表示されます。

システム イベント ログ

システム イベント ログの表示

手順

- ステップ 1** [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2** [Server] タブの [Faults and Logs] をクリックします。
- ステップ 3** [Faults and Logs] ペインの [System Event Log] タブをクリックします。
- ステップ 4** ログ テーブルの上にパーセンテージ バーが表示され、ログ バッファがどれくらい使用されているかが示されます。
- ステップ 5** ログのシステム イベントごとに次の情報を確認します。

名前	説明
[Time] カラム	イベントが発生した日時。
[Severity] カラム	[Severity] フィールドには、テキストと色分けされたアイコンの両方が含まれます。アイコンについては、緑色は通常動作、黄色は情報を示し、警告、クリティカルおよび回復不能なエラーは赤色で表示されます。
[Description] カラム	イベントの説明。
[Clear Log] ボタン	ログ ファイルからすべてのイベントをクリアします。 (注) このオプションは、お使いのユーザ ID に <code>admin</code> または <code>user</code> ロールが割り当てられている場合のみ使用できます。

- ステップ 6** [Entries Per Page] ドロップダウン リストから、各ページに表示するシステム イベントの数を選択します。
- ステップ 7** システム イベントのページを前方および後方に移動するには [<Newer] および [Older>] をクリックし、リストの先頭に移動するには [<<Newest] をクリックします。
デフォルトでは、最新のシステム イベントがリストの先頭に表示されます。

システム イベント ログのクリア

はじめる前に

システム イベント ログをクリアするには、ユーザ権限を持つユーザとしてログインする必要があります。

手順

- ステップ 1 [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2 [Server] タブの [Faults and Logs] をクリックします。
- ステップ 3 [Faults and Logs] ペインの [System Event Log] タブをクリックします。
- ステップ 4 [System Event Log] ペインで、[Clear Log] をクリックします。
- ステップ 5 表示されるダイアログボックスで [OK] をクリックします。

Cisco IMC Log

CIMC ログの表示

手順

- ステップ 1 [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2 [Server] タブの [Faults and Logs] をクリックします。
- ステップ 3 [Faults and Logs] ペインの [Cisco IMC Log] タブをクリックします。
- ステップ 4 ログの CIMC イベントごとに次の情報を確認します。

名前	説明
[Timestamp] カラム	イベントが発生した日時。

名前	説明
[Severity] カラム	イベントの重大度。次のいずれかになります。 <ul style="list-style-type: none"> • [Emergency] • [Alert] • [Critical] • [Error] • [Warning] • [Notice] • [Informational] • [Debug]
[Source] カラム	イベントをログに記録したソフトウェア モジュール。
[Description] カラム	イベントの説明。
[Clear Log] ボタン	ログ ファイルからすべてのイベントをクリアします。 (注) このオプションは、お使いのユーザ ID に admin または user ロールが割り当てられている場合のみ使用できます。

ステップ 5 [Entries Per Page] ドロップダウン リストから、各ページに表示する CIMC イベントの数を選択します。

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

CIMC ログのクリア

はじめる前に

CIMC ログをクリアするには、ユーザ権限を持つユーザとしてログインする必要があります。

手順

- ステップ 1 [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2 [Server] タブの [Faults and Logs] をクリックします。
- ステップ 3 [Faults and Logs] ペインの [Cisco IMC Log] タブをクリックします。
- ステップ 4 [CIMC Log] ペインで、[Clear Log] をクリックします。
- ステップ 5 表示されるダイアログボックスで [OK] をクリックします。

CIMC ログしきい値の設定

CIMC ログに含まれるメッセージの最低レベルを指定できます。

手順

- ステップ 1 [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2 [Server] タブの [Faults and Logs] をクリックします。
- ステップ 3 [Faults and Logs] ペインの [Logging Controls] タブをクリックします。
- ステップ 4 [Local Logging] 領域で、[Minimum Severity to Report] ドロップダウンリストを使用して、CIMC ログに含まれるメッセージの最低レベルを指定します。
次のいずれかを選択できます。重大度の高いものから順に並んでいます。

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

(注) CIMC では、選択した重大度よりも低い重大度のメッセージはログに記録されません。たとえば、[Error] を選択した場合、CIMC ログには重大度が Emergency、Alert、Critical、または Error のすべてのメッセージが含まれます。Warning、Notice、Informational、または Debug のメッセージは表示されません。

リモートサーバへの CIMC ログの送信

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

はじめる前に

- リモート syslog サーバが、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 サーバが、認証関連のログを含め、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が、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

- ステップ 1** [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2** [Server] タブの [Faults and Logs] をクリックします。
- ステップ 3** [Faults and Logs] ペインの [Logging Controls] タブをクリックします。
- ステップ 4** いずれかの [Remote Syslog Server] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Enabled] チェックボックス	オンにすると、CIMC は [IP Address] フィールドに指定された Syslog サーバにログメッセージを送信します。
[IP Address] フィールド	CIMC ログを保存する Syslog サーバの IP アドレス。
[Port] フィールド	1 ~ 65535 の範囲内の Syslog サーバの宛先ポート番号を入力します。デフォルトのポート番号は 514 です。

- ステップ 5** (任意) [Minimum Severity to Report] ドロップダウンリストで、リモート ログに含まれるメッセージの最低レベルを指定します。
次のいずれかを選択できます。重大度の高いものから順に並んでいます。

- [Emergency]
- [Alert]
- [Critical]
- [Error]
- [Warning]
- [Notice]

- [Informational]
- [Debug]

(注) CIMC では、選択した重大度よりも低い重大度のメッセージは、リモートでログに記録されません。たとえば、[Error] を選択した場合、CIMC リモート ログには重大度が Emergency、Alert、Critical、または Error のすべてのメッセージが含まれます。Warning、Notice、Informational、または Debug のメッセージは表示されません。

ステップ 6 [Save Changes] をクリックします。



第 15 章

サーバユーティリティ

この章は、次の項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, 195 ページ](#)
- [CIMC の再起動, 197 ページ](#)
- [CIMC の出荷時デフォルトへのリセット, 198 ページ](#)
- [CIMC 設定のエクスポートとインポート, 199 ページ](#)
- [ログイン バナー ファイルの内容の変更, 202 ページ](#)

テクニカル サポート データのエクスポート

リモート サーバへのテクニカル サポート データのエクスポート

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

手順

- ステップ 1** [Navigation] ペインの [Admin] タブをクリックします。
- ステップ 2** [Admin] タブの [Utilities] をクリックします。
- ステップ 3** [Utilities] ペインの [Actions] 領域で、[Export Technical Support Data to Remote Server] をクリックします。
- ステップ 4** [Export Technical Support Data] ダイアログボックスで、次のフィールドに入力します。

名前	説明
[Export Technical Support Data to] ドロップダウン リスト	<p>リモートサーバのタイプ。次のいずれかになります。</p> <ul style="list-style-type: none"> • [TFTP Server] • [FTP Server] • [SFTP Server] • [SCP Server] • [HTTP Server] <p>(注) 選択したリモートサーバによって、表示されるフィールドが変わります。</p>
[TFTP]、[FTP]、[SFTP]、[SCP]、または [HTTP Server IP/Hostname] フィールド	サポート データ ファイルを保存する必要があるサーバの IP アドレスまたはホスト名。
[Path and Filename] フィールド	ファイルをリモートサーバにエクスポートするとき、CIMC が使用するパスとファイル名。
[Username]	<p>システムがリモートサーバへのログインに使用するユーザ名。</p> <p>(注) このフィールドは、リモートサーバが TFTP または HTTP の場合は表示されません。</p>
[Password]	<p>リモートサーバのユーザ名のパスワード。</p> <p>(注) このフィールドは、リモートサーバが TFTP または HTTP の場合は表示されません。</p>

ステップ 5 [Export] をクリックします。

次の作業

生成されたレポート ファイルを Cisco TAC に提供します。

ローカルファイルへのテクニカルサポートデータのダウンロード

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

手順

- ステップ 1** [Navigation] ペインの [Admin] タブをクリックします。
- ステップ 2** [Admin] タブの [Utilities] をクリックします。
- ステップ 3** [Utilities] ペインの [Actions] 領域で、[Generate Technical Support Data for Local Download] をクリックします。
- ステップ 4** [Download Technical Support Data to Local File] ダイアログボックスで、次のフィールドに入力します。

名前	説明
[Generate Technical Support Data] オプション ボタン	ダウンロードするテクニカル サポート データ ファイルが存在しない場合、CIMC によってこのオプション ボタンが表示されます。 [Generate] をクリックして、データファイルを作成します。データ収集が完了したら、[Actions] 領域の [Download Technical Support Data to Local File] をクリックして、ファイルをダウンロードします。
[Download to local file] オプション ボタン	テクニカル サポート データ ファイルがダウンロード可能な場合、CIMC によってこのオプション ボタンが有効化されます。 既存のファイルをダウンロードするには、このオプションを選択し、[Download] をクリックします。

次の作業

生成されたレポート ファイルを Cisco TAC に提供します。

CIMC の再起動

現在実行されているファームウェアで問題が発生した場合など、非常に珍しいケースですが、サーバのトラブルシューティング時に、CIMC の再起動が必要になることがあります。この手順は、通常のサーバ メンテナンスには含まれません。CIMC を再起動した後にログオフすると、CIMC は数分間使用できません。



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

はじめる前に

CIMC を再起動するには、admin 権限を持つユーザとしてログインする必要があります。

手順

-
- ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
 - ステップ 2 [Admin] タブの [Utilities] をクリックします。
 - ステップ 3 [Utilities] ペインの [Actions] 領域で、[Reboot CIMC] をクリックします。
 - ステップ 4 [OK] をクリックします。
-

CIMC の出荷時デフォルトへのリセット

現在実行されているファームウェアで問題が発生した場合など、非常に珍しいケースですが、サーバのトラブルシューティング時に、CIMC の出荷時デフォルトへのリセットが必要になることがあります。これを行うと、ユーザが設定可能なすべての設定がリセットされます。

この手順は、通常のサーバメンテナンスには含まれません。CIMC をリセットした後は、ログオフしてから再びログインする必要があります。また、接続が失われ、ネットワーク設定を再び指定する必要がある場合もあります。

はじめる前に

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

手順

-
- ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
 - ステップ 2 [Admin] タブの [Utilities] をクリックします。
 - ステップ 3 [Utilities] ペインの [Actions] 領域で、[Reset CIMC to Factory Default Configuration] をクリックします。
 - ステップ 4 [OK] をクリックします。
ホストが BIOS POST（電源投入時自己診断テスト）を実行しているとき、または EFI シェル内にあるときに CIMC を再起動すると、ホストの電源が短時間オフになります。準備ができると、CIMC の電源はオンになります。
-

CIMC 設定のエクスポートとインポート

CIMC 設定のエクスポートとインポート

CIMC 設定のバックアップを実行するには、システム設定のスナップショットを作成し、生成された CIMC 設定ファイルをネットワーク上の場所にエクスポートします。エクスポート操作で保存されるのは、管理プレーンからの情報だけです。サーバ上のデータはバックアップされません。ユーザアカウントやサーバ証明書など、機密情報の設定はエクスポートされません。

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

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

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

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

CIMC 設定のエクスポート



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

はじめる前に

バックアップ TFTP サーバの IP アドレスを取得します。

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

手順

- ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
- ステップ 2 [Admin] タブの [Utilities] をクリックします。
- ステップ 3 [Utilities] ペインの [Actions] 領域で、[Export CIMC Configuration] をクリックします。
- ステップ 4 [Export CIMC Configuration] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Export to a Local File] オプション ボタン	<p>CIMC GUI を実行するコンピュータのローカルドライブに XML 設定ファイルを保存するには、このオプションを選択し、[Export] をクリックします。</p> <p>このオプションを選択すると、CIMC GUI によって [Browse] ダイアログボックスが表示され、設定ファイルを保存する場所への移動が可能になります。</p>
[Export to Remote Server] オプション ボタン	<p>XML 設定ファイルを保存するリモート サーバのタイプ。次のいずれかになります。</p> <ul style="list-style-type: none"> • TFTP サーバ • FTP サーバ • [SFTP Server] • SCP サーバ • HTTP サーバ <p>(注) ドロップダウンリストから選択するリモートサーバによって、表示されるフィールドが変わります。</p> <ul style="list-style-type: none"> • [TFTP]、[FTP]、[SFTP]、[SCP]、または [HTTP Server IP/Hostname] フィールド：設定ファイルを保存するリモートサーバの IP アドレスまたはホスト名。 • [Path and Filename]：設定ファイルを保存するリモートサーバのパスとファイル名。 <p>このファイル名を入力する場合は、サーバツリーの最上位からファイルの場所までのファイルの相対パスを含めてください。</p>

- ステップ 5 [Export] をクリックします。

CIMC 設定のインポート

はじめる前に

コンフィギュレーションファイルのインポート時に SNMP 設定情報を復元する場合は、インポートを行う前にこのサーバで SNMP がディセーブルになっていることを確認します。インポート時に SNMP がイネーブルになっていると、CIMC は現在の値をコンフィギュレーションファイルに保存されている値で上書きしません。

手順

- ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
- ステップ 2 [Admin] タブの [Utilities] をクリックします。
- ステップ 3 [Utilities] ペインの [Actions] 領域で、[Import CIMC Configuration] をクリックします。
- ステップ 4 [Import CIMC Configuration] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Import from a Local File] オプション ボタン	<p>CIMC GUI を実行するコンピュータのローカル ドライブに保存された XML 設定ファイルに移動するには、このオプションを選択し、[Import] をクリックします。</p> <p>このオプションを設定すると、CIMCGUI によって [File] フィールドと [Browse] ボタンが表示され、インポートするファイルへの移動が可能になります。</p>

名前	説明
[Import from Remote Server] オプション ボタン	<p>XML 設定ファイルのインポート元のリモートサーバのタイプ。次のいずれかになります。</p> <ul style="list-style-type: none"> • TFTP サーバ • FTP サーバ • [SFTP Server] • SCP サーバ • HTTP サーバ <p>(注) ドロップダウンリストから選択するリモートサーバによって、表示されるフィールドが変わります。</p> <ul style="list-style-type: none"> • [TFTP]、[FTP]、[SFTP]、[SCP]、または [HTTP Server IP/Hostname] フィールド：設定ファイルが存在するリモートサーバの IP アドレスまたはホスト名。 • [Path and Filename]：設定ファイルのインポート元のリモートサーバのパスとファイル名。 <p>このファイル名を入力する場合は、サーバツリーの最上位からファイルの場所までのファイルの相対パスを含めてください。</p>

ステップ 5 [Import] をクリックします。

ログインバナー ファイルの内容の変更

デフォルトでは、CIMC ログインページにはバナーファイルが含まれています。バナーファイルの内容を変更するには、次の手順を実行します。

手順

- ステップ 1 [Navigation] ペインの [Admin] タブをクリックします。
- ステップ 2 [Admin] タブの [Utilities] をクリックします。
- ステップ 3 [Utilities] ペインの [Actions] 領域で、[Import Login Banner File] をクリックします。
- ステップ 4 [Import Login Banner] ダイアログボックスで、次のフィールドに値を入力します。

名前	説明
[Import from a Local File] オプション ボタン	<p>CIMC GUI を実行するコンピュータのローカル ドライブに保存されたバナーファイルに移動するには、このオプションを選択し、[Import] をクリックします。</p> <p>このオプションを設定すると、CIMC GUI によって [File] フィールドと [Browse] ボタンが表示され、インポートするファイルへの移動が可能になります。</p>
[Import from Remote Server] オプション ボタン	<p>バナーファイルが配置されているリモートサーバのタイプ。次のいずれかになります。</p> <ul style="list-style-type: none"> • TFTP サーバ • FTP サーバ • [SFTP Server] • SCP サーバ • HTTP サーバ <p>(注) ドロップダウンリストから選択するリモートサーバによって、表示されるフィールドが変わります。</p> <ul style="list-style-type: none"> • [TFTP]、[FTP]、[SFTP]、[SCP]、または [HTTP Server IP/Hostname] フィールド：バナーファイルが存在するリモートサーバの IP アドレスまたはホスト名。 • [Path and Filename]：リモートサーバ上のバナーファイルのパスとファイル名。 <p>このファイル名を入力する場合は、サーバツリーの最上位からファイルの場所までのファイルの相対パスを含めてください。</p>

ステップ 5 [Import] をクリックします。



第 16 章

診断テスト

この章は、次の項で構成されています。

- 診断テストの概要, 205 ページ
- ホストへの診断イメージのマッピング, 206 ページ
- 診断テストの実行 : E シリーズ サーバおよび SME シリーズ NCE, 208 ページ
- 診断テストの実行 : EHWIC E シリーズ NCE および NIM E シリーズ NCE, 211 ページ

診断テストの概要

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

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

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



注意

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

診断テストを実行するための基本的なワークフロー

- 1 データをバックアップします。
- 2 診断イメージは購入時にEシリーズサーバまたはNCEに事前にインストールされています。最新の診断イメージを、指定したFTPまたはHTTPサーバからCIMC内部リポジトリにダウンロードすることもできます。
- 3 診断イメージをUSBコントローラのHDD仮想ドライブにマウントします。
- 4 内部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。



(注)

- EシリーズサーバおよびSMEシリーズNCEの場合：サーバのリブート時にEFIシェルが表示されます。
- EHWIC EシリーズNCEおよびNIMEシリーズNCEの場合：サーバのリブート時にAMIDdiag EFIシェルが表示されます。

- 6 必要に応じてEFIシェルまたはAMIDdiag EFIシェルから診断テストを実行します。
- 7 仮想メディアのブート順を元の設定にリセットします。

ホストへの診断イメージのマッピング

はじめる前に

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



(注)

アップデートがすでに処理中であるときにイメージアップデートを開始すると、どちらのアップデートも失敗します。

手順

- ステップ 1** [Navigation] ペインの [Server] メニューをクリックします。
- ステップ 2** [Server] タブの [Host Image Mapping] をクリックします。
- ステップ 3** [Host Image Mapping] ページで、[Add Image] をクリックします。
[Download Image] ダイアログボックスが開きます。次のフィールドに入力します。

名前	説明
[Download Image From] ドロップダウンリスト	イメージが配置されているリモートサーバのタイプ。次のいずれかになります。 <ul style="list-style-type: none"> • FTP • HTTP (注) 選択したリモートサーバによって、表示されるフィールドが変わります。
[FTP] または [HTTP Server IP Address] フィールド	リモート FTP または HTTP サーバの IP アドレス。
[FTP] または [HTTP File Path] フィールド	リモート FTP または HTTP サーバのパスおよびファイル名。 パスワードには、最大 80 文字を使用できます。 <ul style="list-style-type: none"> • ホストイメージをインストールする場合、そのイメージのファイル拡張子は必ず .iso または .img になります。 • 診断イメージをインストールする場合、そのイメージのファイル拡張子は必ず .diag になります。
[Username] フィールド	リモートサーバのユーザ名。 ユーザ名は 1～20 文字の範囲で指定します。 (注) ユーザ名を設定しない場合は、ユーザ名として anonymous を入力し、パスワードとして任意の文字を入力します。
[Password] フィールド	ユーザ名のパスワード。 パスワードは 1～20 文字の範囲で指定します。 (注) ユーザ名を設定しない場合は、ユーザ名として anonymous を入力し、パスワードとして任意の文字を入力します。

- ステップ 4** [Download] をクリックします。

[Host Image Mapping] ページが開きます。[Host Image Mapping Status] 領域で、イメージダウンロードのステータスを表示できます。イメージが正常にダウンロードされ、処理された後、ページがリフレッシュされます。ページがリフレッシュされた後、新しいイメージが [Image Information] 領域に表示されます。

- ステップ 5** [Image Information] 領域で、マップするイメージを選択し、[Map Selected Image] をクリックします。イメージがマップされ、USB コントローラの仮想ドライブにマウントされます。
- ステップ 6** 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。ブート順序の設定については、[CIMC GUI を使用したサーバのブート順の設定](#)、(21 ページ) を参照してください。
- ステップ 7** サーバをリブートします。EFI シェルが表示されます。

次の作業

診断テストを実行します。

診断テストの実行：E シリーズサーバおよびSME シリーズ NCE

EFI シェルから、次の手順を使用してE シリーズ サーバおよびSM E シリーズ NCE で診断テストを実行します。

はじめる前に

- バックアップデータ。テストはすべて非破壊的ですが、テストの実行中に停電や装置の障害が発生すると、ディスクデータが破損する可能性があります。これらのテストを実行する前に、データをバックアップすることを強く推奨します。
- CIMC CLI または CIMC GUI を使用して、診断イメージをダウンロードし、USB コントローラの HDD 仮想ドライブ上にマップします。
- サーバをリブートします。EFI シェルが表示されます。

手順

	コマンドまたはアクション	目的
ステップ 1	Shell > <code>dir virtual-media-drive-name:</code>	指定した仮想メディアドライブ内に存在するすべてのファイルパッケージを表示します。ドライブ名は fs0 から始まり、fs0、fs1、fs2 などがあります。

	コマンドまたはアクション	目的
		(注) 仮想メディア ドライブ名の末尾に必ずコロンを追加してください。例：dir fs1:
ステップ 2	Shell > <i>virtual-media-drive-name</i> :	診断ファイルが保存されている仮想メディア ドライブに移動します。
ステップ 3	Virtual Media Drive :> <i>cp package-file-namedsh.pkg</i>	診断を実行するパッケージファイルを診断シェルパッケージ ファイルにコピーします。
ステップ 4	Virtual Media Drive :> dsh	診断シェルを開始します。確認プロンプトで、y と答えます。
ステップ 5	Server: SRV > run all	<p>使用可能なすべての診断テストを実行し、テストの進行状況とステータスを表示します。診断テストは、サーバの CPU、メモリ、およびブロック デバイス上で実行されます。ブロック デバイスにはハード ドライブ、USB ドライブ、SD カードなどがあります。</p> <p>サーバ上で特定の診断テストを実行するには、run test-name コマンドを使用します。test-name には次のいずれかを指定できます。</p> <ul style="list-style-type: none"> • cpux64 : CPU の診断テスト。 • diskx64 : ブロック デバイスの診断テスト。ブロック デバイスにはハード ドライブ、USB ドライブ、SD カードなどがあります。 • memoryx64 : メモリの診断テスト。 <p>(注) 診断テストの実行には、約 10 分の時間がかかる可能性があります。</p>
ステップ 6	(任意) Server: SRV > results	<p>テスト ステータスが Passed または Failed の診断テストのサマリーを表示します。</p> <p>(注) このサマリー レポートは、失敗および合格したテストの数を示します。どのテストが失敗または合格したかについての情報は提供しません。失敗および合格したテストを判別するには、run all コマンドの出力を確認してください。</p>
ステップ 7	(任意) Server: SRV > show	サーバ上で管理されていたグローバル パラメータと診断テスト モジュールの一覧を表示します。
ステップ 8	Server: SRV > exit	診断シェルを終了します。

	コマンドまたはアクション	目的
ステップ 9	Cisco TAC でサービス要求を開きます。	<p>診断テストに合格した場合、サーバの CPU、メモリ、ブロック デバイスに問題はありません。他のハードウェアコンポーネントまたはソフトウェア設定に問題がある可能性があります。Cisco TAC でサービス要求を開いて、問題を特定します。</p> <p>診断テストが失敗した場合は、Cisco TAC でサービス要求を開いて支援を求めます。</p>

次の例では、すべての診断テストを実行しています。

```
Shell > dir fs1:
 06/27/12 07:48p          1,435,424  Dsh.efi
 06/27/12 08:03p           10,036  dsh-e140d.pkg
 06/25/12 06:00p           10,140  dsh-e140s.pkg
 06/27/12 08:04p           10,042  dsh-e160d.pkg
    4 File(s)    1,465,642 bytes

Shell > fs1:
fs1:\> cp dsh-e140d.pkg dsh.pkg
copying fs0:\OBD\dsh-e140d.pkg -> fs0:\OBD\dsh.pkg
- [ok]
fs1:\> dsh
Diagnostics is a standalone utility that runs on the server module independent
of the operating system or applications running on the module.All tests are
non-destructive, but there is a possibility of disk data corruption 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。

診断テストの実行：EHWIC E シリーズ NCE および NIM E シリーズ NCE

診断テストは、サーバの CPU、メモリ、およびブロックデバイス上で実行されます。ブロックデバイスには SSD ドライブおよび USB ドライブが含まれます。

はじめる前に

- バックアップデータ。テストはすべて非破壊的ですが、テストの実行中に停電や装置の障害が発生すると、ディスクデータが破損する可能性があります。これらのテストを実行する前に、データをバックアップすることを強く推奨します。
- AMIDIAG_OBD.log ファイルの以前のバージョンがある場合は、それを削除します。
- CIMC CLI または CIMC GUI を使用して、診断イメージをダウンロードし、USB コントローラの HDD 仮想ドライブ上にマップします。
- KVM コンソールを起動します。
- サーバをリブートします。KVM コンソールに AMIDIag EFI シェルが表示されます。

```
Found AMI DIAG on fs0:
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 data corruption 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
```

```
Enter 'q' to quit, any other key to continue:
```

```
fs0:\>
```

手順

	コマンドまたはアクション	目的
ステップ 1	AMIDIag EFI シェルから、 (q 以外の) 任意のキーを押して診断テストを実行します。	有効なすべての診断テストが実行され、進捗が表示されます。テストが完了すると、テストステータスとして Pass または Fail が表示されます。 (注) 診断テストの実行には、約 10 分の時間がかかる可能性があります。
ステップ 2	(任意) fs0:\> type AMIDIAG_OBD.log	詳細な Onboard Diag ログファイルが表示されます。
ステップ 3	Server: fs0:\> exit	AMIDIag EFI シェルを終了します。
ステップ 4	Cisco TAC でサービス要求を開きます。	診断テストに合格した場合、サーバの CPU、メモリ、ブロックデバイスに問題はありません。他の

	コマンドまたはアクション	目的
		ハードウェア コンポーネントまたはソフトウェア設定に問題がある可能性があります。Cisco TAC でサービス要求を開いて、問題を特定します。 診断テストが失敗した場合は、Cisco TAC でサービス要求を開いて支援を求めます。

次の作業

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

記号

- [Navigation] ペイン [6](#)
- [Server] タブ [6](#)
- [Work] ペイン [6](#)

A

- Active Directory [132](#)
- \ [6](#)

B

- BIOS [32, 36, 176, 177, 182, 183](#)
 - CMOS [36](#)
 - クリア [36](#)
 - password [36](#)
 - クリア [36](#)
 - アクティブ化 [32](#)
 - シスコからのファームウェアの取得 [177](#)
 - シスコのオプションからのファームウェアの取得 [176](#)
 - バックアップ [32](#)
 - アクティブ化 [32](#)
 - ファームウェア [182, 183](#)
 - TFTP サーバからのインストール [183](#)
 - ブラウザ経由のインストール [182](#)
- BIOS CMOS [36](#)
 - クリア [36](#)
- BIOS セットアップ [24](#)
- BIOS パスワード [36](#)
 - クリア [36](#)
- BIOS ファームウェア [182, 183](#)
 - TFTP サーバからのインストール [183](#)
 - ブラウザ経由のインストール [182](#)
- BIOS 設定 [32, 34, 37](#)
 - advanced [32](#)

BIOS 設定 (続き)

- サーバ管理 [34](#)
- 概要 [37](#)
- BOOTX64.EFI [88](#)
 - RAID ボリューム [88](#)

C

- CIMC [175, 176, 177, 178, 180, 181, 189, 190, 191, 192, 197, 198](#)
 - ファームウェア [178, 180, 181](#)
 - アクティブ化 [181](#)
 - ブラウザ経由のインストール [180](#)
 - リモートサーバからのインストール [178](#)
 - ファームウェアの概要 [175](#)
 - リポート [197](#)
 - ログしきい値の設定 [191](#)
 - ログのクリア [190](#)
 - ログの送信 [192](#)
 - ログの表示 [189](#)
 - 出荷時の初期状態へのリセット [198](#)
- CIMC GUI [4, 5](#)
- CIMC GUI の使用 [21](#)
- CIMC NIC [141](#)
- CIMC の概要 [3](#)
- CIMC ファームウェア [180, 181](#)
 - アクティブ化 [181](#)
 - ブラウザ経由のインストール [180](#)
- cimc マップされた vmedia ボリューム [125](#)
 - 作成 [125](#)
- CIMC マップされた vmedia ボリューム [129](#)
 - 削除 [129](#)
- CIMC マップされた vMedia ボリューム [128](#)
 - プロパティ [128](#)
- CIMC 情報 [104](#)
- CPU プロパティ [105](#)

EE シリーズ サーバ [1](#)概要 [1](#)events [169, 170](#)platform [169, 170](#)アラートのイネーブル化 [169](#)アラートのディセーブル化 [170](#)**H**HTTP プロパティ [151](#)**I**IOS 設定変更 [26](#)locking [26](#)ロック解除 [26](#)IP ブロッキング [146](#)IPMI over LAN [154](#)設定 [154](#)説明 [154](#)IPv4 プロパティ [145](#)**K**KVM [122, 123, 124](#)イネーブル化 [122, 123](#)ディセーブル化 [124](#)設定 [122](#)KVM コンソール [10, 121](#)KVM のイネーブル化 [122, 123](#)KVM のディセーブル化 [124](#)**L**LDAP [134](#)設定 [134](#)LDAP サーバ [133](#)LED センサー [117](#)LOM のプロパティ [112](#)**M**MAC address [112](#)interface [112](#)**N**NCE [1](#)概要 [1](#)NIC プロパティ [142](#)NTP 設定 [148](#)NTP 設定の構成 [148](#)**O**OS のインストール [9, 11, 13](#)KVM コンソール [11](#)PXE [13](#)方法 [9](#)**P**PCI アダプタ [111](#)プロパティの表示 [111](#)PXE インストール [13](#)**R**RAID [58, 59](#)設定の削除 [59](#)変更、設定の [58](#)RAID オプション [52](#)RAID の容量 [71](#)CIMC GUI の使用 [71](#)RAID、設定 [55](#)CIMC GUI の使用 [55](#)**S**Serial over LAN [129](#)SNMP [156, 159, 161](#)SNMPv3 ユーザの管理 [161](#)SNMPv3 ユーザの設定 [159](#)テストトラップメッセージの送信 [159](#)プロパティの設定 [156](#)

SSH プロパティ [152](#)
 syslog [192](#)
 CIMC ログの送信 [192](#)

T

TPM [49](#)

U

UEFI [88](#)
 CIMC GUI の使用 [88](#)

V

VLAN プロパティ [146](#)
 VMware [14](#)
 ソフトウェアの取得 [14](#)

W

W2K12 [70](#)

X

XML API [153](#)
 説明 [153](#)
 XML API プロパティ [153](#)

あ

アダプタ [111](#)
 PCI [111](#)

い

イベントフィルタ、プラットフォーム [169, 170](#)
 概要 [169](#)
 設定 [170](#)
 イベント ログ、システム [188, 189](#)
 クリア [189](#)
 表示 [188](#)

インポート [201](#)
 CIMC 設定 [201](#)

え

エクスポート [199](#)
 CIMC 設定 [199](#)

お

オペレーティング システムのインストール [11](#)

こ

コミュニケーションサービスのプロパティ [151, 152, 153, 154](#)
 HTTP プロパティ [151](#)
 IPMI over LAN プロパティ [154](#)
 SSH プロパティ [152](#)
 XML API プロパティ [153](#)

さ

サーバソフトウェア [2](#)
 サーバヘルス [19](#)
 サーバのシャットダウン [25](#)
 サーバのプロパティ [103](#)
 サーバのリセット [25](#)
 サーバの電源オフ [27](#)
 サーバの電源投入 [27](#)
 サーバ管理 [19, 21, 25, 27, 28, 148](#)
 NTP 設定の構成 [148](#)
 サーバヘルス [19](#)
 サーバのシャットダウン [25](#)
 サーバのリセット [25](#)
 サーバの電源オフ [27](#)
 サーバの電源投入 [27](#)
 サーバ電源の再投入 [28](#)
 ブート順の設定 [21](#)
 サーバ証明書のアップロード [167](#)
 サーバ電源の再投入 [28](#)

し

システム イベント ログ **188, 189**
 クリア **189**
 表示 **188**

す

ストレージ センサー **118**
 ストレージのプロパティ **109**
 表示 **109**

せ

センサー **115, 116, 117, 118**
 LED **117**
 temperature **115**
 ストレージ **118**
 電圧 **116**

そ

ソフトウェア **14**
 VMware からの取得 **14**

つ

ツールバー **7**

て

テクニカル サポート データ **195, 196**
 リモート サーバへのエクスポート **195**
 ローカル ファイルへのダウンロード **196**

と

トラップ設定 **157**
 設定 **157**

ね

ネットワーク セキュリティ **147**
 ネットワーク プロパティ **142, 144, 145, 146**
 IPv4 プロパティ **145**
 NIC プロパティ **142**
 VLAN プロパティ **146**
 共通プロパティ **144**
 ネットワーク解析機能の有効化 **148**
 ネットワーク接続 **113**
 status **113**

は

バックアップ **199**
 CIMC 設定 **199**

ふ

ファームウェア **175, 176, 177, 178**
 アップグレード **176**
 シスコからの取得 **177**
 リモート サーバからのインストール **178**
 概要 **175**
 ブート可能なディスク ドライブ **68**
 CIMC GUI の使用 **68**
 ブート順、設定 **21**
 ブート順の設定 **24**
 プラットフォーム イベント **169, 170, 171**
 アラートのイネーブル化 **169**
 アラートのディセーブル化 **170**
 トラップの解釈 **171**
 プラットフォーム イベント フィルタ **169, 170**
 概要 **169**
 設定 **170**
 フロッピーディスクのエミュレーション **124**

ほ

ホスト イメージ **15, 17, 18**
 マッピング解除 **17**
 削除 **18**
 ホスト イメージ、マッピング **15**

ま

マッピング [15](#)

め

メモリのプロパティ [106](#)

ゆ

ユーザ セッション [139](#)

ユーザ管理 [131](#), [134](#), [139](#)

LDAP [134](#)

ユーザ セッション [139](#)

ローカル ユーザ [131](#)

り

リセット ボタン [31](#)

locking [31](#)

リセット ボタン (続き)

ロック解除 [31](#)

リモート プレゼンス [122](#), [123](#), [124](#), [129](#)

Serial over LAN [129](#)

仮想 KVM [122](#), [123](#), [124](#)

仮想メディア [124](#)

リンク ステート [113](#)

る

ルータ情報 [105](#)

ろ

ローカル ユーザ [131](#)

ログアウト [8](#)

ログイン [4](#)

ログイン バナー [202](#)

インポート [202](#)

